National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 - 15 Oct 2022 Vol. 09 No. 19

Table of Content

Vendor	Product	Page Number
Dell	chengming_3990	938
	chengming_3991	941
	edge_gateway_3000	943
	edge_gateway_5000	946
	embedded_box_pc_3000	949
	embedded_box_pc_5000	952
	g3_15_3590	954
	g3_15_5590	957
	g3_3579	960
	g3_3779	963
	g5_5000	965
	g5_5090	968
	g7_17_7590	971
	g7_17_7790	974
	inspiron_14_3467	976
	inspiron_15_2-in-1_5582	979
	inspiron_15_3567	982
	inspiron_3277	984
	inspiron_3280	987
	inspiron_3470	990
	inspiron_3471	993
	inspiron_3477	995
	inspiron_3480	998
	inspiron_3481	1001
	inspiron_3482	1004
	inspiron_3490	1006
	inspiron_3493	1009
	inspiron_3501	1012
	inspiron_3502	1015
	inspiron_3580	1017
	inspiron_3581	1020
	inspiron_3582	1023

Vendor	Product	Page Number
Dell	inspiron_3590	1025
	inspiron_3593	1028
	inspiron_3670	1031
	inspiron_3671	1034
	inspiron_3780	1036
	inspiron_3781	1039
	inspiron_3782	1042
	inspiron_3790	1045
	inspiron_3793	1047
	inspiron_3880	1050
	inspiron_3881	1053
	inspiron_5390	1056
	inspiron_5391	1058
	inspiron_5400	1061
	inspiron_5401	1064
	inspiron_5477	1066
	inspiron_5480	1069
	inspiron_5481	1072
	inspiron_5482	1075
	inspiron_5490	1077
	inspiron_5491_2-in-1	1080
	inspiron_5491_aio	1083
	inspiron_5493	1086
	inspiron_5494	1088
	inspiron_5498	1091
	inspiron_5570	1094
	inspiron_5580	1097
	inspiron_5583	1099
	inspiron_5584	1102
	inspiron_5590	1105
	inspiron_5591_2-in-1	1107
	inspiron_5593	1110

Vendor	Product	Page Number
Dell	inspiron_5594	1113
	inspiron_5598	1116
	inspiron_5680	1118
	inspiron_5770	1121
	inspiron_7000	1124
	inspiron_7370	1127
	inspiron_7373	1129
	inspiron_7380	1132
	inspiron_7386	1135
	inspiron_7390	1138
	inspiron_7391	1140
	inspiron_7490	1143
	inspiron_7570	1146
	inspiron_7573	1148
	inspiron_7580	1151
	inspiron_7586	1154
	inspiron_7590	1157
	inspiron_7591	1159
	inspiron_7700_aio	1162
	inspiron_7777	1165
	inspiron_7786	1168
	inspiron_7790	1170
	inspiron_7791	1173
	latitude_3120	1176
	latitude_3180	1179
	latitude_3189	1181
	latitude_3190	1184
	latitude_3190_2-in-1	1187
	latitude_3300	1189
	latitude_3301	1192
	latitude_3310	1195
	latitude_3310_2-in-1	1198

Vendor	Product	Page Number
Dell	latitude_3379	1200
	latitude_3390	1203
	latitude_3420	1206
	latitude_3480	1206
	latitude_3490	1209
	latitude_3580	1212
	latitude_3590	1214
	latitude_5280	1217
	latitude_5285_2-in-1	1220
	latitude_5289	1223
	latitude_5290	1225
	latitude_5290_2-in-1	1228
	latitude_5300	1231
	latitude_5300_2-in-1	1234
	latitude_5310	1236
	latitude_5310_2-in-1	1239
	latitude_5400	1242
	latitude_5401	1245
	latitude_5410	1247
	latitude_5411	1250
	latitude_5414_rugged	1253
	latitude_5420_rugged	1255
	latitude_5480	1258
	latitude_5488	1261
	latitude_5490	1264
	latitude_5491	1266
	latitude_5495	1269
	latitude_5500	1272
	latitude_5501	1275
	latitude_5510	1277
	latitude_5511	1280
	latitude_5580	1283

Vendor	Product	Page Number
Dell	latitude_5590	1286
	latitude_5591	1288
	latitude_7200_2-in-1	1291
	latitude_7210_2-in-1	1294
	latitude_7212_rugged_extreme_tablet	1296
	latitude_7214_rugged_extreme	1299
	latitude_7220ex_rugged_extreme_tablet	1302
	latitude_7220_rugged_extreme_tablet	1305
	latitude_7275_2-in-1	1307
	latitude_7290	1310
	latitude_7300	1313
	latitude_7310	1316
	latitude_7370	1318
	latitude_7380	1321
	latitude_7389	1324
	latitude_7390	1327
	latitude_7390_2-in-1	1329
	latitude_7400	1332
	latitude_7400_2-in-1	1335
	latitude_7410	1337
	latitude_7414_rugged_extreme	1340
	latitude_7424_rugged_extreme	1343
	latitude_7480	1346
	latitude_7490	1348
	latitude_9410	1351
	latitude_9510	1354
	latitude_e5270	1357
	latitude_e5470	1359
	latitude_e5570	1362
	latitude_e7270	1365
	latitude_e7470	1368
	optiplex_3000_thin_client	1370

Vendor	Product	Page Number
Dell	optiplex_3040	1371
	optiplex_3046	1373
	optiplex_3050	1376
	optiplex_3050_aio	1379
	optiplex_3060	1382
	optiplex_3070	1384
	optiplex_3080	1387
	optiplex_3090	1390
	optiplex_3280_aio	1393
	optiplex_5050	1395
	optiplex_5055	1398
	optiplex_5060	1401
	optiplex_5070	1403
	optiplex_5080	1406
	optiplex_5260_all-in-one	1409
	optiplex_5480_all-in-one	1412
	optiplex_7040	1414
	optiplex_7050	1417
	optiplex_7060	1420
	optiplex_7070	1423
	optiplex_7070_ultra	1425
	optiplex_7071	1428
	optiplex_7080	1431
	optiplex_7450	1434
	optiplex_7460_all_in_one	1436
	optiplex_7470_all-in-one	1439
	optiplex_7480_all-in-one	1442
	optiplex_xe3	1444
	precision_3240_compact	1447
	precision_3420_tower	1450
	precision_3430_tower	1453
	precision_3431_tower	1455

Vendor	Product	Page Number
Dell	precision_3440	1458
	precision_3510	1461
	precision_3520	1464
	precision_3540	1466
	precision_3541	1469
	precision_3550	1472
	precision_3551	1475
	precision_3620_tower	1477
	precision_3630_tower	1480
	precision_3640_tower	1483
	precision_3930_rack	1485
	precision_5510	1488
	precision_5530	1491
	precision_5530_2-in-1	1494
	precision_5540	1496
	precision_5720_aio	1499
	precision_5820_tower	1502
	precision_7510	1505
	precision_7520	1508
	precision_7530	1511
	precision_7540	1513
	precision_7550	1516
	precision_7710	1519
	precision_7720	1522
	precision_7730	1524
	precision_7740	1527
	precision_7750	1530
	precision_7820_tower	1533
	precision_7920_tower	1536
	vostro_3070	1539
	vostro_3267	1542
	vostro_3268	1545

Vendor	Product	Page Number
Dell	wyse_5470	1630
	wyse_5470_all-in-one	1633
	wyse_5470_all-in-one_thin_client	1636
	wyse_5470_mobile_thin_client	1636
	wyse_7040_thin_client	1637
	xps_13_7390	1639
	xps_13_7390_2-in-1	1642
	xps_13_9300	1645
	xps_13_9365_2-in-1	1647
	xps_13_9370	1650
	xps_13_9380	1653
	xps_15_7590	1656
	xps_15_9575_2-in-1	1658
	xps_7590	1661
	xps_8930	1664
	xps_8940	1667
	xps_8950	1669
	xtremio_x1	1672
	xtremio_x2	1672
foresightsports	gc3_launch_monitor	1673
generex	cs141	1674
mediabridgeproducts	mlwr-ac1200r	1674
mediatek	mt6580	1675
	mt6739	1676
	mt6753	1677
	mt6757	1678
	mt6761	1678
	mt6762	1681
	mt6763	1683
	mt6765	1684
	mt6768	1687
	mt6769	1689

Vendor	Product	Page Number
mediatek	mt6771	1691
	mt6779	1691
	mt6781	1693
	mt6785	1696
	mt6789	1699
	mt6833	1702
	mt6853	1705
	mt6853t	1707
	mt6855	1709
	mt6873	1713
	mt6875	1715
	mt6877	1717
	mt6879	1720
	mt6883	1724
	mt6885	1726
	mt6889	1729
	mt6891	1731
	mt6893	1733
	mt6895	1735
	mt6983	1739
	mt7663	1744
	mt7668	1745
	mt7902	1746
	mt7921	1748
	mt8167s	1749
	mt8168	1750
	mt8175	1751
	mt8183	1752
	mt8185	1754
	mt8321	1755
	mt8362a	1757
	mt8365	1759

Vendor	Product	Page Number
Siemens	6gk5205-3bb00-2tb2	1801
	6gk5205-3bd00-2ab2	1801
	6gk5205-3bd00-2tb2	1801
	6gk5205-3bf00-2ab2	1802
	6gk5205-3bf00-2tb2	1802
	6gk5206-2bb00-2ac2	1803
	6gk5206-2bd00-2ac2	1803
	6gk5206-2bs00-2ac2	1803
	6gk5206-2bs00-2fc2	1804
	6gk5206-2gs00-2ac2	1804
	6gk5206-2gs00-2fc2	1804
	6gk5206-2gs00-2tc2	1805
	6gk5206-2rs00-2ac2	1805
	6gk5206-2rs00-5ac2	1805
	6gk5206-2rs00-5fc2	1806
	6gk5208-0ba00-2ab2	1806
	6gk5208-0ba00-2ac2	1806
	6gk5208-0ba00-2fc2	1807
	6gk5208-0ba00-2tb2	1807
	6gk5208-0ga00-2ac2	1807
	6gk5208-0ga00-2fc2	1808
	6gk5208-0ga00-2tc2	1808
	6gk5208-0ha00-2as6	1809
	6gk5208-0ha00-2es6	1809
	6gk5208-0ha00-2ts6	1809
	6gk5208-0ra00-2ac2	1810
	6gk5208-0ra00-5ac2	1810
	6gk5208-0ua00-5es6	1810
	6gk5213-3bb00-2ab2	1811
	6gk5213-3bb00-2tb2	1811
	6gk5213-3bd00-2ab2	1811
	6gk5213-3bd00-2tb2	1812

Vendor	Product	Page Number
Siemens	6gk5213-3bf00-2ab2	1812
	6gk5213-3bf00-2tb2	1812
	6gk5216-0ba00-2ab2	1813
	6gk5216-0ba00-2ac2	1813
	6gk5216-0ba00-2fc2	1813
	6gk5216-0ba00-2tb2	1814
	6gk5216-0ha00-2as6	1814
	6gk5216-0ha00-2es6	1815
	6gk5216-0ha00-2ts6	1815
	6gk5216-0ua00-5es6	1815
	6gk5216-3rs00-2ac2	1816
	6gk5216-3rs00-5ac2	1816
	6gk5216-4bs00-2ac2	1816
	6gk5216-4gs00-2ac2	1817
	6gk5216-4gs00-2fc2	1817
	6gk5216-4gs00-2tc2	1817
	6gk5224-0ba00-2ac2	1818
	6gk5224-4gs00-2ac2	1818
	6gk5224-4gs00-2fc2	1818
	6gk5224-4gs00-2tc2	1819
	6gk5324-0ba00-2ar3	1819
	6gk5324-0ba00-3ar3	1819
	6gk5326-2qs00-3ar3	1820
	6gk5326-2qs00-3rr3	1820
	6gk5328-4fs00-2ar3	1821
	6gk5328-4fs00-2rr3	1821
	6gk5328-4fs00-3ar3	1821
	6gk5328-4fs00-3rr3	1822
	6gk5328-4ss00-2ar3	1822
	6gk5328-4ss00-3ar3	1822
	6gk5408-4gp00-2am2	1823
	6gk5408-4gq00-2am2	1823

Vendor	Product	Page Number
Siemens	6gk5408-8gr00-2am2	1823
	6gk5408-8gs00-2am2	1824
	6gk5416-4gr00-2am2	1824
	6gk5416-4gs00-2am2	1824
	6gk5524-8gr00-2ar2	1825
	6gk5524-8gr00-3ar2	1825
	6gk5524-8gr00-4ar2	1825
	6gk5524-8gs00-2ar2	1826
	6gk5524-8gs00-3ar2	1826
	6gk5524-8gs00-4ar2	1827
	6gk5526-8gr00-2ar2	1827
	6gk5526-8gr00-3ar2	1827
	6gk5526-8gr00-4ar2	1828
	6gk5526-8gs00-2ar2	1828
	6gk5526-8gs00-3ar2	1828
	6gk5526-8gs00-4ar2	1829
	6gk5528-0aa00-2ar2	1829
	6gk5528-0aa00-2hr2	1829
	6gk5528-0ar00-2ar2	1830
	6gk5528-0ar00-2hr2	1830
	6gk5552-0aa00-2ar2	1830
	6gk5552-0aa00-2hr2	1831
	6gk5552-0ar00-2ar2	1831
	6gk5552-0ar00-2hr2	1831
	6gk5622-2gs00-2ac2	1832
	6gk5632-2gs00-2ac2	1832
	6gk5636-2gs00-2ac2	1833
	6gk5642-2gs00-2ac2	1833
	6gk5646-2gs00-2ac2	1833
	6gk5721-1fc00-0aa0	1834
	6gk5721-1fc00-0ab0	1834
	6gk5722-1fc00-0aa0	1834

Vendor	Product	Page Number
Siemens	6gk5722-1fc00-0ab0	1835
	6gk5722-1fc00-0ac0	1835
	6gk5734-1fx00-0aa0	1835
	6gk5734-1fx00-0aa6	1836
	6gk5734-1fx00-0ab0	1836
	6gk5734-1fx00-0ab6	1836
	6gk5738-1gy00-0aa0	1837
	6gk5738-1gy00-0ab0	1837
	6gk5748-1fc00-0aa0	1837
	6gk5748-1fc00-0ab0	1838
	6gk5748-1gd00-0aa0	1838
	6gk5748-1gd00-0ab0	1839
	6gk5748-1gy01-0aa0	1839
	6gk5748-1gy01-0ta0	1839
	6gk5761-1fc00-0aa0	1840
	6gk5761-1fc00-0ab0	1840
	6gk5763-1al00-3aa0	1840
	6gk5763-1al00-3da0	1841
	6gk5763-1al00-7da0	1841
	6gk5766-1ge00-3da0	1841
	6gk5766-1ge00-3db0	1842
	6gk5766-1ge00-7da0	1842
	6gk5766-1ge00-7db0	1842
	6gk5766-1ge00-7ta0	1843
	6gk5766-1ge00-7tb0	1843
	6gk5766-1je00-3da0	1843
	6gk5766-1je00-7da0	1844
	6gk5766-1je00-7ta0	1844
	6gk5774-1fx00-0aa0	1845
	6gk5774-1fx00-0aa6	1845
	6gk5774-1fx00-0ab0	1845
	6gk5774-1fx00-0ab6	1846

Vendor	Product	Page Number
Siemens	6gk5774-1fx00-0ac0	1846
	6gk5774-1fy00-0ta0	1846
	6gk5774-1fy00-0tb0	1847
	6gk5778-1gy00-0aa0	1847
	6gk5778-1gy00-0ab0	1847
	6gk5778-1gy00-0ta0	1848
	6gk5778-1gy00-0tb0	1848
	6gk5786-1fc00-0aa0	1848
	6gk5786-1fc00-0ab0	1849
	6gk5786-2fc00-0aa0	1849
	6gk5786-2fc00-0ab0	1849
	6gk5786-2fc00-0ac0	1850
	6gk5786-2fe00-0aa0	1850
	6gk5786-2fe00-0ab0	1851
	6gk5786-2hc00-0aa0	1851
	6gk5786-2hc00-0ab0	1851
	6gk5788-1fc00-0aa0	1852
	6gk5788-1fc00-0ab0	1852
	6gk5788-1gd00-0aa0	1852
	6gk5788-1gd00-0ab0	1853
	6gk5788-1gy01-0aa0	1853
	6gk5788-2fc00-0aa0	1853
	6gk5788-2fc00-0ab0	1854
	6gk5788-2fc00-0ac0	1854
	6gk5788-2gd00-0aa0	1854
	6gk5788-2gd00-0ab0	1855
	6gk5788-2gd00-0ta0	1855
	6gk5788-2gd00-0tb0	1855
	6gk5788-2gd00-0tc0	1856
	6gk5788-2gy01-0aa0	1856
	6gk5788-2gy01-0ta0	1857
	6gk5788-2hy01-0aa0	1857

Vendor	Product	Page Number
Siemens	6gk5804-0ap00-2aa2	1857
	6gk5812-1aa00-2aa2	1858
	6gk5812-1ba00-2aa2	1858
	6gk5816-1aa00-2aa2	1858
	6gk5816-1ba00-2aa2	1859
	6gk5826-2ab00-2ab2	1859
	6gk5853-2ea00-2da1	1859
	6gk5856-2ea00-3aa1	1860
	6gk5856-2ea00-3da1	1860
	6gk5874-2aa00-2aa2	1860
	6gk5874-3aa00-2aa2	1861
	6gk5876-3aa02-2ba2	1861
	6gk5876-3aa02-2ea2	1861
	6gk5876-4aa00-2ba2	1862
	6gk5876-4aa00-2da2	1862
	6gk6108-4am00-2ba2	1863
	6gk6108-4am00-2da2	1863
	7kg8500-0aa00-0aa0	1863
	7kg8500-0aa00-2aa0	1867
	7kg8500-0aa10-0aa0	1871
	7kg8500-0aa10-2aa0	1876
	7kg8500-0aa30-0aa0	1880
	7kg8500-0aa30-2aa0	1884
	7kg8501-0aa01-0aa0	1888
	7kg8501-0aa01-2aa0	1892
	7kg8501-0aa02-0aa0	1896
	7kg8501-0aa02-2aa0	1900
	7kg8501-0aa11-0aa0	1905
	7kg8501-0aa11-2aa0	1909
	7kg8501-0aa12-0aa0	1913
	7kg8501-0aa12-2aa0	1917
	7kg8501-0aa31-0aa0	1921

Vendor	Product	Page Number
Siemens	7kg8501-0aa31-2aa0	1925
	7kg8501-0aa32-0aa0	1929
	7kg8501-0aa32-2aa0	1934
	7kg8550-0aa00-0aa0	1938
	7kg8550-0aa00-2aa0	1942
	7kg8550-0aa10-0aa0	1946
	7kg8550-0aa10-2aa0	1950
	7kg8550-0aa30-0aa0	1954
	7kg8550-0aa30-2aa0	1958
	7kg8551-0aa01-0aa0	1963
	7kg8551-0aa01-2aa0	1967
	7kg8551-0aa02-0aa0	1971
	7kg8551-0aa02-2aa0	1975
	7kg8551-0aa11-0aa0	1979
	7kg8551-0aa11-2aa0	1983
	7kg8551-0aa12-0aa0	1987
	7kg8551-0aa12-2aa0	1992
	7kg8551-0aa31-0aa0	1996
	7kg8551-0aa31-2aa0	2000
	7kg8551-0aa32-0aa0	2004
	7kg8551-0aa32-2aa0	2008
	apogee_modular_building_controller	2012
	apogee_modular_equiment_controller	2013
	apogee_pxc_compact	2014
	apogee_pxc_modular	2014
	desigo_pxc00-e.d	2015
	desigo_pxc00-u	2016
	desigo_pxc001-e.d	2017
	desigo_pxc100-e.d	2017
	desigo_pxc12-e.d	2018
	desigo_pxc128-u	2019
	desigo_pxc200-e.d	2019

Vendor	Product	Page Number
Siemens	desigo_pxc22-e.d	2020
	desigo_pxc22.1-e.d	2021
	desigo_pxc36.1-e.d	2022
	desigo_pxc50-e.d	2022
	desigo_pxc64-u	2023
	desigo_pxm20-e	2024
	desigo_pxm30-1	2024
	desigo_pxm30.e	2034
	desigo_pxm40-1	2043
	desigo_pxm40.e	2053
	desigo_pxm50-1	2062
	desigo_pxm50.e	2072
	logo\!8_bm	2081
	logo\!8_bm_fs-05	2083
	pxg3.w100-1	2085
	pxg3.w100-2	2095
	pxg3.w200-1	2104
	pxg3.w200-2	2114
	ruggedcom_rm1224	2123
	scalance_m804pb	2126
	scalance_m812-1	2129
	scalance_m816-1	2131
	scalance_m826-2	2134
	scalance_m874-2	2136
	scalance_m874-3	2139
	scalance_m876-3	2142
	scalance_m876-4	2144
	scalance_mum853-1	2147
	scalance_mum856-1	2150
	scalance_s615	2152
	scalance_wam763-1	2155
	scalance_wam766-1	2158

Vendor	Product	Page Number
Siemens	scalance_wum763-1	2160
	scalance_wum766-1	2163
	scalance_x200-4p_irt	2166
	scalance_x201-3p_irt	2168
	scalance_x201-3p_irt_pro	2170
	scalance_x202-2irt	2172
	scalance_x202-2p_irt	2174
	scalance_x202-2p_irt_pro	2176
	scalance_x204-2	2179
	scalance_x204-2fm	2181
	scalance_x204-2ld	2183
	scalance_x204-2ld_ts	2185
	scalance_x204-2ts	2187
	scalance_x204irt	2189
	scalance_x204irt_pro	2192
	scalance_x206-1	2194
	scalance_x206-1ld	2196
	scalance_x208	2198
	scalance_x208pro	2200
	scalance_x212-2	2202
	scalance_x212-2ld	2205
	scalance_x216	2207
	scalance_x224	2209
	scalance_xf201-3p_irt	2211
	scalance_xf202-2p_irt	2213
	scalance_xf204	2215
	scalance_xf204-2	2218
	scalance_xf204-2ba_irt	2220
	scalance_xf204irt	2222
	scalance_xf206-1	2224
	scalance_xf208	2226
	simatic_drive_controller_cpu_1504d_tf	2228

Vendor	Product	Page Number
Siemens	simatic_drive_controller_cpu_1507d_tf	2230
	simatic_et_200_open_controller_cpu_1515sp_pc	2232
	simatic_et_200_open_controller_cpu_1515sp_pc2	2233
	simatic_hmi_comfort_panels	2235
	simatic_hmi_ktp1200_basic	2236
	simatic_hmi_ktp400_basic	2238
	simatic_hmi_ktp700_basic	2239
	simatic_hmi_ktp900_basic	2240
	simatic_hmi_ktp_mobile_panels	2242
	simatic_s7-1200_cpu_12_1211c	2243
	simatic_s7-1200_cpu_12_1212c	2245
	simatic_s7-1200_cpu_12_1212fc	2246
	simatic_s7-1200_cpu_12_1214c	2248
	simatic_s7-1200_cpu_12_1214fc	2250
	simatic_s7-1200_cpu_12_1215c	2251
	simatic_s7-1200_cpu_12_1215fc	2253
	simatic_s7-1200_cpu_12_1217c	2255
	simatic_s7-1500_cpu_1510sp	2256
	simatic_s7-1500_cpu_1510sp-1	2258
	simatic_s7-1500_cpu_1511-1	2260
	simatic_s7-1500_cpu_1511t-1	2261
	simatic_s7-1500_cpu_1511tf-1	2263
	simatic_s7-1500_cpu_1512c-1	2265
	simatic_s7-1500_cpu_1512sp-1	2267
	simatic_s7-1500_cpu_1512spf-1	2268
	simatic_s7-1500_cpu_1513-1	2270
	simatic_s7-1500_cpu_1513f-1	2272
	simatic_s7-1500_cpu_1513r-1	2273
	simatic_s7-1500_cpu_1515-2	2275
	simatic_s7-1500_cpu_151511c-1	2277
	simatic_s7-1500_cpu_151511f-1	2278

Vendor	Product	Page Number
Siemens	simatic_s7-1500_cpu_1515f-2	2280
	simatic_s7-1500_cpu_1515r-2	2282
	simatic_s7-1500_cpu_1515t-2	2283
	simatic_s7-1500_cpu_1516-3	2285
	simatic_s7-1500_cpu_1516f-3	2287
	simatic_s7-1500_cpu_1516pro_f	2288
	simatic_s7-1500_cpu_1516t-3	2290
	simatic_s7-1500_cpu_1516tf-3	2292
	simatic_s7-1500_cpu_1517-3	2293
	simatic_s7-1500_cpu_1517f-3	2295
	simatic_s7-1500_cpu_1518-4	2297
	simatic_s7-1500_cpu_1518f-4	2299
	simatic_s7-1500_cpu_1518hf-4	2300
	simatic_s7-1500_cpu_1518t-4	2302
	simatic_s7-1500_cpu_1518tf-4	2304
	simatic_s7-1500_cpu_15pro-2	2305
	simatic_s7-1500_cpu_15prof-2	2307
	simatic_s7-plcsim_advanced	2309
	siplus_hmi_ktp1200_basic	2310
	siplus_hmi_ktp400_basic	2312
	siplus_hmi_ktp700_basic	2313
	siplus_hmi_ktp900_basic	2314
	siplus_net_scalance_x202-2p_irt	2316
	talon_tc_compact	2318
Tenda	ac1206	2318
	ax1803	2320
totolink	nr1800x	2321
wayos	lq-04	2325
	lq-05	2325
	lq-06	2326
	lq-07	2326
	lq-08	2327

Vendor	Product	Page Number
Dell	alienware_x15_r2_firmware	2464
	alienware_x17_r1_firmware	2467
	alienware_x17_r2_firmware	2469
	bios	2472
	chengming_3980_firmware	2473
	chengming_3988_firmware	2476
	chengming_3990_firmware	2479
	chengming_3991_firmware	2482
	edge_gateway_3000_firmware	2484
	edge_gateway_5000_firmware	2487
	embedded_box_pc_3000_firmware	2490
	embedded_box_pc_5000_firmware	2493
	enterprise_sonic_distribution	2495
	g3_15_3590_firmware	2496
	g3_15_5590_firmware	2499
	g3_3579_firmware	2502
	g3_3779_firmware	2504
	g5_5000_firmware	2507
	g5_5090_firmware	2510
	g7_17_7590_firmware	2513
	g7_17_7790_firmware	2515
	inspiron_14_3467_firmware	2518
	inspiron_15_2-in-1_5582_firmware	2521
	inspiron_15_3567_firmware	2523
	inspiron_3277_firmware	2526
	inspiron_3280_firmware	2529
	inspiron_3470_firmware	2532
	inspiron_3471_firmware	2534
	inspiron_3477_firmware	2537
	inspiron_3480_firmware	2540
	inspiron_3481_firmware	2543
	inspiron_3482_firmware	2545

Vendor	Product	Page Number
Dell	inspiron_3490_firmware	2548
	inspiron_3493_firmware	2551
	inspiron_3501_firmware	2554
	inspiron_3502_firmware	2556
	inspiron_3580_firmware	2559
	inspiron_3581_firmware	2562
	inspiron_3582_firmware	2564
	inspiron_3590_firmware	2567
	inspiron_3593_firmware	2570
	inspiron_3670_firmware	2573
	inspiron_3671_firmware	2575
	inspiron_3780_firmware	2578
	inspiron_3781_firmware	2581
	inspiron_3782_firmware	2584
	inspiron_3790_firmware	2586
	inspiron_3793_firmware	2589
	inspiron_3880_firmware	2592
	inspiron_3881_firmware	2595
	inspiron_5390_firmware	2597
	inspiron_5391_firmware	2600
	inspiron_5400_firmware	2603
	inspiron_5401_firmware	2605
	inspiron_5477_firmware	2608
	inspiron_5480_firmware	2611
	inspiron_5481_firmware	2614
	inspiron_5482_firmware	2616
	inspiron_5490_firmware	2619
	inspiron_5491_2-in-1_firmware	2622
	inspiron_5491_aio_firmware	2625
	inspiron_5493_firmware	2627
	inspiron_5494_firmware	2630
	inspiron_5498_firmware	2633

Vendor	Product	Page Number
Dell	inspiron_5570_firmware	2636
	inspiron_5580_firmware	2638
	inspiron_5583_firmware	2641
	inspiron_5584_firmware	2644
	inspiron_5590_firmware	2646
	inspiron_5591_2-in-1_firmware	2649
	inspiron_5593_firmware	2652
	inspiron_5594_firmware	2655
	inspiron_5598_firmware	2657
	inspiron_5680_firmware	2660
	inspiron_5770_firmware	2663
	inspiron_7000_firmware	2666
	inspiron_7370_firmware	2668
	inspiron_7373_firmware	2671
	inspiron_7380_firmware	2674
	inspiron_7386_firmware	2677
	inspiron_7390_firmware	2679
	inspiron_7391_firmware	2682
	inspiron_7490_firmware	2685
	inspiron_7570_firmware	2687
	inspiron_7573_firmware	2690
	inspiron_7580_firmware	2693
	inspiron_7586_firmware	2696
	inspiron_7590_firmware	2698
	inspiron_7591_firmware	2701
	inspiron_7700_aio_firmware	2704
	inspiron_7777_firmware	2707
	inspiron_7786_firmware	2709
	inspiron_7790_firmware	2712
	inspiron_7791_firmware	2715
	latitude_3120_firmware	2718
	latitude_3180_firmware	2720

Vendor	Product	Page Number
Dell	latitude_3189_firmware	2723
	latitude_3190_2-in-1_firmware	2726
	latitude_3190_firmware	2728
	latitude_3300_firmware	2731
	latitude_3301_firmware	2734
	latitude_3310_2-in-1_firmware	2737
	latitude_3310_firmware	2739
	latitude_3379_firmware	2742
	latitude_3390_firmware	2745
	latitude_3480_firmware	2748
	latitude_3490_firmware	2750
	latitude_3580_firmware	2753
	latitude_3590_firmware	2756
	latitude_5280_firmware	2759
	latitude_5285_2-in-1_firmware	2761
	latitude_5289_firmware	2764
	latitude_5290_2-in-1_firmware	2767
	latitude_5290_firmware	2769
	latitude_5300_2-in-1_firmware	2772
	latitude_5300_firmware	2775
	latitude_5310_2-in-1_firmware	2778
	latitude_5310_firmware	2780
	latitude_5400_firmware	2783
	latitude_5401_firmware	2786
	latitude_5410_firmware	2789
	latitude_5411_firmware	2791
	latitude_5414_rugged_firmware	2794
	latitude_5420_rugged_firmware	2797
	latitude_5480_firmware	2800
	latitude_5488_firmware	2802
	latitude_5490_firmware	2805
	latitude_5491_firmware	2808

Vendor	Product	Page Number
Dell	latitude_5495_firmware	2810
	latitude_5500_firmware	2813
	latitude_5501_firmware	2816
	latitude_5510_firmware	2819
	latitude_5511_firmware	2821
	latitude_5580_firmware	2824
	latitude_5590_firmware	2827
	latitude_5591_firmware	2830
	latitude_7200_2-in-1_firmware	2832
	latitude_7210_2-in-1_firmware	2835
	latitude_7212_rugged_extreme_tablet_firmware	2838
	latitude_7214_rugged_extreme_firmware	2841
	latitude_7220ex_rugged_extreme_tablet_firmware	2843
	latitude_7220_rugged_extreme_tablet_firmware	2846
	latitude_7275_2-in-1_firmware	2849
	latitude_7290_firmware	2851
	latitude_7300_firmware	2854
	latitude_7310_firmware	2857
	latitude_7370_firmware	2860
	latitude_7380_firmware	2862
	latitude_7389_firmware	2865
	latitude_7390_2-in-1_firmware	2868
	latitude_7390_firmware	2871
	latitude_7400_2-in-1_firmware	2873
	latitude_7400_firmware	2876
	latitude_7410_firmware	2879
	latitude_7414_rugged_extreme_firmware	2882
	latitude_7424_rugged_extreme_firmware	2884
	latitude_7480_firmware	2887
	latitude_7490_firmware	2890

Vendor	Product	Page Number
Dell	latitude_9410_firmware	2892
	latitude_9510_firmware	2895
	latitude_e5270_firmware	2898
	latitude_e5470_firmware	2901
	latitude_e5570_firmware	2903
	latitude_e7270_firmware	2906
	latitude_e7470_firmware	2909
	optiplex_3040_firmware	2912
	optiplex_3046_firmware	2914
	optiplex_3050_aio_firmware	2917
	optiplex_3050_firmware	2920
	optiplex_3060_firmware	2923
	optiplex_3070_firmware	2925
	optiplex_3080_firmware	2928
	optiplex_3090_firmware	2931
	optiplex_3280_aio_firmware	2933
	optiplex_5050_firmware	2936
	optiplex_5055_firmware	2939
	optiplex_5060_firmware	2942
	optiplex_5070_firmware	2944
	optiplex_5080_firmware	2947
	optiplex_5260_all-in-one_firmware	2950
	optiplex_5480_all-in-one_firmware	2953
	optiplex_7040_firmware	2955
	optiplex_7050_firmware	2958
	optiplex_7060_firmware	2961
	optiplex_7070_firmware	2964
	optiplex_7070_ultra_firmware	2966
	optiplex_7071_firmware	2969
	optiplex_7080_firmware	2972
	optiplex_7450_firmware	2974
	optiplex_7460_all_in_one_firmware	2977

Vendor	Product	Page Number
Dell	optiplex_7470_all-in-one_firmware	2980
	optiplex_7480_all-in-one_firmware	2983
	optiplex_xe3_firmware	2985
	precision_3240_compact_firmware	2988
	precision_3420_tower_firmware	2991
	precision_3430_tower_firmware	2994
	precision_3431_tower_firmware	2996
	precision_3440_firmware	2999
	precision_3510_firmware	3002
	precision_3520_firmware	3005
	precision_3540_firmware	3007
	precision_3541_firmware	3010
	precision_3550_firmware	3013
	precision_3551_firmware	3015
	precision_3620_tower_firmware	3018
	precision_3630_tower_firmware	3021
	precision_3640_tower_firmware	3024
	precision_3930_rack_firmware	3026
	precision_5510_firmware	3029
	precision_5530_2-in-1_firmware	3032
	precision_5530_firmware	3035
	precision_5540_firmware	3037
	precision_5720_aio_firmware	3040
	precision_5820_tower_firmware	3043
	precision_7510_firmware	3046
	precision_7520_firmware	3048
	precision_7530_firmware	3051
	precision_7540_firmware	3054
	precision_7550_firmware	3056
	precision_7710_firmware	3059
	precision_7720_firmware	3062
	precision_7730_firmware	3065

Vendor	Product	Page Number
Dell	precision_7740_firmware	3067
	precision_7750_firmware	3070
	precision_7820_tower_firmware	3073
	precision_7920_tower_firmware	3076
	vostro_3070_firmware	3078
	vostro_3267_firmware	3081
	vostro_3268_firmware	3084
	vostro_3401_firmware	3087
	vostro_3470_firmware	3089
	vostro_3471_firmware	3092
	vostro_3480_firmware	3095
	vostro_3481_firmware	3097
	vostro_3490_firmware	3100
	vostro_3501_firmware	3103
	vostro_3580_firmware	3106
	vostro_3581_firmware	3108
	vostro_3582_firmware	3111
	vostro_3583_firmware	3114
	vostro_3584_firmware	3117
	vostro_3590_firmware	3119
	vostro_3667_firmware	3122
	vostro_3668_firmware	3125
	vostro_3669_firmware	3128
	vostro_3670_firmware	3130
	vostro_3671_firmware	3133
	vostro_3681_firmware	3136
	vostro_3881_firmware	3138
	vostro_3888_firmware	3141
	vostro_5090_firmware	3144
	vostro_5390_firmware	3147
	vostro_5391_firmware	3149
	vostro_5581_firmware	3152

Vendor	Product	Page Number
Microsoft	storsimple_8010_firmware	3285
	storsimple_8020_firmware	3285
	windows	3285
	windows_10	3294
	windows_11	3379
	windows_7	3409
	windows_8.1	3420
	windows_rt_8.1	3432
	windows_server_2008	3444
	windows_server_2012	3467
	windows_server_2016	3491
	windows_server_2019	3504
	windows_server_2022	3519
Nokia	airframe_bmc_web_gui_r18_firmware	3535
Opensuse	leap	3536
	leap_micro	3538
Paloaltonetworks	pan-os	3539
Siemens	6ag1206-2bb00-7ac2_firmware	3539
	6ag1206-2bs00-7ac2_firmware	3540
	6ag1208-0ba00-7ac2_firmware	3540
	6ag1216-4bs00-7ac2_firmware	3540
	6gk5204-0ba00-2gf2_firmware	3541
	6gk5204-0ba00-2yf2_firmware	3541
	6gk5204-2aa00-2gf2_firmware	3541
	6gk5204-2aa00-2yf2_firmware	3542
	6gk5205-3bb00-2ab2_firmware	3542
	6gk5205-3bb00-2tb2_firmware	3543
	6gk5205-3bd00-2ab2_firmware	3543
	6gk5205-3bd00-2tb2_firmware	3543
	6gk5205-3bf00-2ab2_firmware	3544
	6gk5205-3bf00-2tb2_firmware	3544
	6gk5206-2bb00-2ac2_firmware	3544

Vendor	Product	Page Number
Siemens	6gk5206-2bd00-2ac2_firmware	3545
	6gk5206-2bs00-2ac2_firmware	3545
	6gk5206-2bs00-2fc2_firmware	3545
	6gk5206-2gs00-2ac2_firmware	3546
	6gk5206-2gs00-2fc2_firmware	3546
	6gk5206-2gs00-2tc2_firmware	3546
	6gk5206-2rs00-2ac2_firmware	3547
	6gk5206-2rs00-5ac2_firmware	3547
	6gk5206-2rs00-5fc2_firmware	3547
	6gk5208-0ba00-2ab2_firmware	3548
	6gk5208-0ba00-2ac2_firmware	3548
	6gk5208-0ba00-2fc2_firmware	3549
	6gk5208-0ba00-2tb2_firmware	3549
	6gk5208-0ga00-2ac2_firmware	3549
	6gk5208-0ga00-2fc2_firmware	3550
	6gk5208-0ga00-2tc2_firmware	3550
	6gk5208-0ha00-2as6_firmware	3550
	6gk5208-0ha00-2es6_firmware	3551
	6gk5208-0ha00-2ts6_firmware	3551
	6gk5208-0ra00-2ac2_firmware	3551
	6gk5208-0ra00-5ac2_firmware	3552
	6gk5208-0ua00-5es6_firmware	3552
	6gk5213-3bb00-2ab2_firmware	3552
	6gk5213-3bb00-2tb2_firmware	3553
	6gk5213-3bd00-2ab2_firmware	3553
	6gk5213-3bd00-2tb2_firmware	3553
	6gk5213-3bf00-2ab2_firmware	3554
	6gk5213-3bf00-2tb2_firmware	3554
	6gk5216-0ba00-2ab2_firmware	3555
	6gk5216-0ba00-2ac2_firmware	3555
	6gk5216-0ba00-2fc2_firmware	3555
	6gk5216-0ba00-2tb2_firmware	3556

Vendor	Product	Page Number
Siemens	6gk5216-0ha00-2as6_firmware	3556
	6gk5216-0ha00-2es6_firmware	3556
	6gk5216-0ha00-2ts6_firmware	3557
	6gk5216-0ua00-5es6_firmware	3557
	6gk5216-3rs00-2ac2_firmware	3557
	6gk5216-3rs00-5ac2_firmware	3558
	6gk5216-4bs00-2ac2_firmware	3558
	6gk5216-4gs00-2ac2_firmware	3558
	6gk5216-4gs00-2fc2_firmware	3559
	6gk5216-4gs00-2tc2_firmware	3559
	6gk5224-0ba00-2ac2_firmware	3559
	6gk5224-4gs00-2ac2_firmware	3560
	6gk5224-4gs00-2fc2_firmware	3560
	6gk5224-4gs00-2tc2_firmware	3561
	6gk5324-0ba00-2ar3_firmware	3561
	6gk5324-0ba00-3ar3_firmware	3561
	6gk5326-2qs00-3ar3_firmware	3562
	6gk5326-2qs00-3rr3_firmware	3562
	6gk5328-4fs00-2ar3_firmware	3562
	6gk5328-4fs00-2rr3_firmware	3563
	6gk5328-4fs00-3ar3_firmware	3563
	6gk5328-4fs00-3rr3_firmware	3563
	6gk5328-4ss00-2ar3_firmware	3564
	6gk5328-4ss00-3ar3_firmware	3564
	6gk5408-4gp00-2am2_firmware	3564
	6gk5408-4gq00-2am2_firmware	3565
	6gk5408-8gr00-2am2_firmware	3565
	6gk5408-8gs00-2am2_firmware	3565
	6gk5416-4gr00-2am2_firmware	3566
	6gk5416-4gs00-2am2_firmware	3566
	6gk5524-8gr00-2ar2_firmware	3567
	6gk5524-8gr00-3ar2_firmware	3567

Vendor	Product	Page Number
Siemens	6gk5524-8gr00-4ar2_firmware	3567
	6gk5524-8gs00-2ar2_firmware	3568
	6gk5524-8gs00-3ar2_firmware	3568
	6gk5524-8gs00-4ar2_firmware	3568
	6gk5526-8gr00-2ar2_firmware	3569
	6gk5526-8gr00-3ar2_firmware	3569
	6gk5526-8gr00-4ar2_firmware	3569
	6gk5526-8gs00-2ar2_firmware	3570
	6gk5526-8gs00-3ar2_firmware	3570
	6gk5526-8gs00-4ar2_firmware	3570
	6gk5528-0aa00-2ar2_firmware	3571
	6gk5528-0aa00-2hr2_firmware	3571
	6gk5528-0ar00-2ar2_firmware	3571
	6gk5528-0ar00-2hr2_firmware	3572
	6gk5552-0aa00-2ar2_firmware	3572
	6gk5552-0aa00-2hr2_firmware	3573
	6gk5552-0ar00-2ar2_firmware	3573
	6gk5552-0ar00-2hr2_firmware	3573
	6gk5622-2gs00-2ac2_firmware	3574
	6gk5632-2gs00-2ac2_firmware	3574
	6gk5636-2gs00-2ac2_firmware	3574
	6gk5642-2gs00-2ac2_firmware	3575
	6gk5646-2gs00-2ac2_firmware	3575
	6gk5721-1fc00-0aa0_firmware	3575
	6gk5721-1fc00-0ab0_firmware	3576
	6gk5722-1fc00-0aa0_firmware	3576
	6gk5722-1fc00-0ab0_firmware	3576
	6gk5722-1fc00-0ac0_firmware	3577
	6gk5734-1fx00-0aa0_firmware	3577
	6gk5734-1fx00-0aa6_firmware	3577
	6gk5734-1fx00-0ab0_firmware	3578
	6gk5734-1fx00-0ab6_firmware	3578

Vendor	Product	Page Number
Siemens	6gk5738-1gy00-0aa0_firmware	3579
	6gk5738-1gy00-0ab0_firmware	3579
	6gk5748-1fc00-0aa0_firmware	3579
	6gk5748-1fc00-0ab0_firmware	3580
	6gk5748-1gd00-0aa0_firmware	3580
	6gk5748-1gd00-0ab0_firmware	3580
	6gk5748-1gy01-0aa0_firmware	3581
	6gk5748-1gy01-0ta0_firmware	3581
	6gk5761-1fc00-0aa0_firmware	3581
	6gk5761-1fc00-0ab0_firmware	3582
	6gk5763-1al00-3aa0_firmware	3582
	6gk5763-1al00-3da0_firmware	3582
	6gk5763-1al00-7da0_firmware	3583
	6gk5766-1ge00-3da0_firmware	3583
	6gk5766-1ge00-3db0_firmware	3583
	6gk5766-1ge00-7da0_firmware	3584
	6gk5766-1ge00-7db0_firmware	3584
	6gk5766-1ge00-7ta0_firmware	3585
	6gk5766-1ge00-7tb0_firmware	3585
	6gk5766-1je00-3da0_firmware	3585
	6gk5766-1je00-7da0_firmware	3586
	6gk5766-1je00-7ta0_firmware	3586
	6gk5774-1fx00-0aa0_firmware	3586
	6gk5774-1fx00-0aa6_firmware	3587
	6gk5774-1fx00-0ab0_firmware	3587
	6gk5774-1fx00-0ab6_firmware	3587
	6gk5774-1fx00-0ac0_firmware	3588
	6gk5774-1fy00-0ta0_firmware	3588
	6gk5774-1fy00-0tb0_firmware	3588
	6gk5778-1gy00-0aa0_firmware	3589
	6gk5778-1gy00-0ab0_firmware	3589
	6gk5778-1gy00-0ta0_firmware	3589

Vendor	Product	Page Number
Siemens	6gk5778-1gy00-0tb0_firmware	3590
	6gk5786-1fc00-0aa0_firmware	3590
	6gk5786-1fc00-0ab0_firmware	3591
	6gk5786-2fc00-0aa0_firmware	3591
	6gk5786-2fc00-0ab0_firmware	3591
	6gk5786-2fc00-0ac0_firmware	3592
	6gk5786-2fe00-0aa0_firmware	3592
	6gk5786-2fe00-0ab0_firmware	3592
	6gk5786-2hc00-0aa0_firmware	3593
	6gk5786-2hc00-0ab0_firmware	3593
	6gk5788-1fc00-0aa0_firmware	3593
	6gk5788-1fc00-0ab0_firmware	3594
	6gk5788-1gd00-0aa0_firmware	3594
	6gk5788-1gd00-0ab0_firmware	3594
	6gk5788-1gy01-0aa0_firmware	3595
	6gk5788-2fc00-0aa0_firmware	3595
	6gk5788-2fc00-0ab0_firmware	3595
	6gk5788-2fc00-0ac0_firmware	3596
	6gk5788-2gd00-0aa0_firmware	3596
	6gk5788-2gd00-0ab0_firmware	3597
	6gk5788-2gd00-0ta0_firmware	3597
	6gk5788-2gd00-0tb0_firmware	3597
	6gk5788-2gd00-0tc0_firmware	3598
	6gk5788-2gy01-0aa0_firmware	3598
	6gk5788-2gy01-0ta0_firmware	3598
	6gk5788-2hy01-0aa0_firmware	3599
	6gk5804-0ap00-2aa2_firmware	3599
	6gk5812-1aa00-2aa2_firmware	3599
	6gk5812-1ba00-2aa2_firmware	3600
	6gk5816-1aa00-2aa2_firmware	3600
	6gk5816-1ba00-2aa2_firmware	3600
	6gk5826-2ab00-2ab2_firmware	3601

Vendor	Product	Page Number
Siemens	6gk5853-2ea00-2da1_firmware	3601
	6gk5856-2ea00-3aa1_firmware	3601
	6gk5856-2ea00-3da1_firmware	3602
	6gk5874-2aa00-2aa2_firmware	3602
	6gk5874-3aa00-2aa2_firmware	3603
	6gk5876-3aa02-2ba2_firmware	3603
	6gk5876-3aa02-2ea2_firmware	3603
	6gk5876-4aa00-2ba2_firmware	3604
	6gk5876-4aa00-2da2_firmware	3604
	6gk6108-4am00-2ba2_firmware	3604
	6gk6108-4am00-2da2_firmware	3605
	7kg8500-0aa00-0aa0_firmware	3605
	7kg8500-0aa00-2aa0_firmware	3609
	7kg8500-0aa10-0aa0_firmware	3613
	7kg8500-0aa10-2aa0_firmware	3617
	7kg8500-0aa30-0aa0_firmware	3622
	7kg8500-0aa30-2aa0_firmware	3626
	7kg8501-0aa01-0aa0_firmware	3630
	7kg8501-0aa01-2aa0_firmware	3634
	7kg8501-0aa02-0aa0_firmware	3638
	7kg8501-0aa02-2aa0_firmware	3642
	7kg8501-0aa11-0aa0_firmware	3646
	7kg8501-0aa11-2aa0_firmware	3651
	7kg8501-0aa12-0aa0_firmware	3655
	7kg8501-0aa12-2aa0_firmware	3659
	7kg8501-0aa31-0aa0_firmware	3663
	7kg8501-0aa31-2aa0_firmware	3667
	7kg8501-0aa32-0aa0_firmware	3671
	7kg8501-0aa32-2aa0_firmware	3675
	7kg8550-0aa00-0aa0_firmware	3680
	7kg8550-0aa00-2aa0_firmware	3684
	7kg8550-0aa10-0aa0_firmware	3688

Vendor	Product	Page Number
Siemens	7kg8550-0aa10-2aa0_firmware	3692
	7kg8550-0aa30-0aa0_firmware	3696
	7kg8550-0aa30-2aa0_firmware	3700
	7kg8551-0aa01-0aa0_firmware	3704
	7kg8551-0aa01-2aa0_firmware	3709
	7kg8551-0aa02-0aa0_firmware	3713
	7kg8551-0aa02-2aa0_firmware	3717
	7kg8551-0aa11-0aa0_firmware	3721
	7kg8551-0aa11-2aa0_firmware	3725
	7kg8551-0aa12-0aa0_firmware	3729
	7kg8551-0aa12-2aa0_firmware	3733
	7kg8551-0aa31-0aa0_firmware	3738
	7kg8551-0aa31-2aa0_firmware	3742
	7kg8551-0aa32-0aa0_firmware	3746
	7kg8551-0aa32-2aa0_firmware	3750
	apogee_modular_building_controller_firmware	3754
	apogee_modular_equiment_controller_firmware	3755
	apogee_pxc_compact_firmware	3756
	apogee_pxc_modular_firmware	3756
	desigo_pxc00-e.d_firmware	3757
	desigo_pxc00-u_firmware	3758
	desigo_pxc001-e.d_firmware	3758
	desigo_pxc100-e.d_firmware	3759
	desigo_pxc12-e.d_firmware	3760
	desigo_pxc128-u_firmware	3761
	desigo_pxc200-e.d_firmware	3761
	desigo_pxc22-e.d_firmware	3762
	desigo_pxc22.1-e.d_firmware	3763
	desigo_pxc36.1-e.d_firmware	3763
	desigo_pxc50-e.d_firmware	3764
	desigo_pxc64-u_firmware	3765

Vendor	Product	Page Number
Siemens	desigo_pxm20-e_firmware	3766
	desigo_pxm30-1_firmware	3766
	desigo_pxm30.e_firmware	3776
	desigo_pxm40-1_firmware	3785
	desigo_pxm40.e_firmware	3795
	desigo_pxm50-1_firmware	3804
	desigo_pxm50.e_firmware	3814
	logo\!8_bm_fs-05_firmware	3823
	logo\!_8_bm_firmware	3825
	pxg3.w100-1_firmware	3827
	pxg3.w100-2_firmware	3837
	pxg3.w200-1_firmware	3846
	pxg3.w200-2_firmware	3856
	ruggedcom_rm1224_firmware	3865
	scalance_m804pb_firmware	3868
	scalance_m812-1_firmware	3870
	scalance_m816-1_firmware	3873
	scalance_m826-2_firmware	3876
	scalance_m874-2_firmware	3878
	scalance_m874-3_firmware	3881
	scalance_m876-3_firmware	3884
	scalance_m876-4_firmware	3886
	scalance_mum853-1_firmware	3889
	scalance_mum856-1_firmware	3891
	scalance_s615_firmware	3894
	scalance_wam763-1_firmware	3897
	scalance_wam766-1_firmware	3899
	scalance_wum763-1_firmware	3902
	scalance_wum766-1_firmware	3905
	scalance_x200-4p_irt_firmware	3907
	scalance_x201-3p_irt_firmware	3910
	scalance_x201-3p_irt_pro_firmware	3912

Vendor	Product	Page Number
Siemens	scalance_x202-2irt_firmware	3914
	scalance_x202-2p_irt_firmware	3916
	scalance_x202-2p_irt_pro_firmware	3918
	scalance_x204-2fm_firmware	3920
	scalance_x204-2ld_firmware	3923
	scalance_x204-2ld_ts_firmware	3925
	scalance_x204-2ts_firmware	3927
	scalance_x204-2_firmware	3929
	scalance_x204irt_firmware	3931
	scalance_x204irt_pro_firmware	3933
	scalance_x206-1ld_firmware	3936
	scalance_x206-1_firmware	3938
	scalance_x208pro_firmware	3940
	scalance_x208_firmware	3942
	scalance_x212-2ld_firmware	3944
	scalance_x212-2_firmware	3946
	scalance_x216_firmware	3949
	scalance_x224_firmware	3951
	scalance_xf201-3p_irt_firmware	3953
	scalance_xf202-2p_irt_firmware	3955
	scalance_xf204-2ba_irt_firmware	3957
	scalance_xf204-2_firmware	3959
	scalance_xf204irt_firmware	3962
	scalance_xf204_firmware	3964
	scalance_xf206-1_firmware	3966
	scalance_xf208_firmware	3968
	simatic_drive_controller_cpu_1504d_tf_firmware	3970
	simatic_drive_controller_cpu_1507d_tf_firmware	3972
	simatic_et_200_sp_open_controller_cpu_1515sp_pc2_firmware	3974

Vendor	Product	Page Number
Siemens	simatic_et_200_sp_open_controller_cpu_1515sp_pc_firmware	3975
	simatic_hmi_comfort_panels_firmware	3977
	simatic_hmi_ktp1200_basic_firmware	3980
	simatic_hmi_ktp400_basic_firmware	3982
	simatic_hmi_ktp700_basic_firmware	3985
	simatic_hmi_ktp900_basic_firmware	3987
	simatic_hmi_ktp_mobile_panels_firmware	3990
	simatic_s7-1200_cpu_12_1211c_firmware	3992
	simatic_s7-1200_cpu_12_1212c_firmware	3994
	simatic_s7-1200_cpu_12_1212fc_firmware	3996
	simatic_s7-1200_cpu_12_1214c_firmware	3998
	simatic_s7-1200_cpu_12_1214fc_firmware	3999
	simatic_s7-1200_cpu_12_1215c_firmware	4001
	simatic_s7-1200_cpu_12_1215fc_firmware	4003
	simatic_s7-1200_cpu_12_1217c_firmware	4004
	simatic_s7-1500_cpu_1510sp-1_firmware	4006
	simatic_s7-1500_cpu_1510sp_firmware	4008
	simatic_s7-1500_cpu_1511-1_firmware	4009
	simatic_s7-1500_cpu_1511t-1_firmware	4011
	simatic_s7-1500_cpu_1511tf-1_firmware	4013
	simatic_s7-1500_cpu_1512c-1_firmware	4014
	simatic_s7-1500_cpu_1512sp-1_firmware	4016
	simatic_s7-1500_cpu_1512spf-1_firmware	4018
	simatic_s7-1500_cpu_1513-1_firmware	4019
	simatic_s7-1500_cpu_1513f-1_firmware	4021
	simatic_s7-1500_cpu_1513r-1_firmware	4023
	simatic_s7-1500_cpu_1515-2_firmware	4024
	simatic_s7-1500_cpu_151511c-1_firmware	4026
	simatic_s7-1500_cpu_151511f-1_firmware	4028
	simatic_s7-1500_cpu_1515f-2_firmware	4030
	simatic_s7-1500_cpu_1515r-2_firmware	4031
	simatic_s7-1500_cpu_1515t-2_firmware	4033

Vendor	Product	Page Number
Siemens	simatic_s7-1500_cpu_1516-3_firmware	4035
	simatic_s7-1500_cpu_1516f-3_firmware	4036
	simatic_s7-1500_cpu_1516pro_f_firmware	4038
	simatic_s7-1500_cpu_1516t-3_firmware	4040
	simatic_s7-1500_cpu_1516tf-3_firmware	4041
	simatic_s7-1500_cpu_1517-3_firmware	4043
	simatic_s7-1500_cpu_1517f-3_firmware	4045
	simatic_s7-1500_cpu_1518-4_firmware	4046
	simatic_s7-1500_cpu_1518f-4_firmware	4048
	simatic_s7-1500_cpu_1518hf-4_firmware	4050
	simatic_s7-1500_cpu_1518t-4_firmware	4051
	simatic_s7-1500_cpu_1518tf-4_firmware	4053
	simatic_s7-1500_cpu_15pro-2_firmware	4055
	simatic_s7-1500_cpu_15prof-2_firmware	4056
	simatic_s7-plcsim_advanced_firmware	4058
	siplus_hmi_ktp1200_basic_firmware	4060
	siplus_hmi_ktp400_basic_firmware	4062
	siplus_hmi_ktp700_basic_firmware	4065
	siplus_hmi_ktp900_basic_firmware	4068
	siplus_net_scalance_x202-2p_irt_firmware	4070
	talon_tc_compact_firmware	4072
Suse	linux_enterprise_server	4073
Tenda	ac1206_firmware	4074
	ax1803_firmware	4076
totolink	nr1800x_firmware	4076
Vmware	esxi	4080
wayos	lq-04_firmware	4081
	lq-05_firmware	4081
	lq-06_firmware	4082
	lq-07_firmware	4082
	lq-08_firmware	4083
	lq-09_firmware	4083

Vendor	Product	Page Number
wijungle	u250_firmware	4084
XEN	xapi	4084
	xen	4085

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: adguard					
Product: adguardhome					
Affected Version(s): 0.108					
Cross-Site Request Forgery (CSRF)	11-Oct-2022	4.3	In AdGuardHome, versions v0.95 through v0.108.0-b.13 are vulnerable to Cross-Site Request Forgery (CSRF), in the custom filtering rules functionality. An attacker can persuade an authorized user to follow a malicious link, resulting in deleting/modifying the custom filtering rules. **CVE ID : CVE-2022-32175**	N/A	A-ADG-ADGU-201022/1
Affected Version(s): From (including) 0.95 Up to (excluding) 0.108					
Cross-Site Request Forgery (CSRF)	11-Oct-2022	4.3	In AdGuardHome, versions v0.95 through v0.108.0-b.13 are vulnerable to Cross-Site Request Forgery (CSRF), in the custom filtering rules functionality. An attacker can persuade an authorized user to follow a malicious link, resulting in deleting/modifying	N/A	A-ADG-ADGU-201022/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the custom filtering rules. **CVE ID : CVE-2022-32175**		
Vendor: Apache					
Product: airflow					
Affected Version(s): * Up to (including) 2.4.1					
Insufficient Session Expiration	07-Oct-2022	8.1	In Apache Airflow, prior to version 2.4.1, deactivating a user wouldn't prevent an already authenticated user from being able to continue using the UI or API. **CVE ID : CVE-2022-41672**	https://github.com/apache/airflow/pull/26635, https://lists.apache.org/thread/ohf3pvd3dftb8zb01yngbn1jtkq5m08y	A-APA-AIRF-201022/3
Product: commons_jxpath					
Affected Version(s): * Up to (including) 1.3					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	06-Oct-2022	9.8	Those using JXPath to interpret untrusted XPath expressions may be vulnerable to a remote code execution attack. All JXPathContext class functions processing a XPath string are vulnerable except compile() and compilePath() function. The XPath expression can be used by an attacker to load any Java class from the classpath resulting in code execution.	N/A	A-APA-COMM-201022/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41852		
Out-of-bounds Write	06-Oct-2022	6.5	Those using JXPath to interpret XPath may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40157**	N/A	A-APA-COMM-201022/5
Out-of-bounds Write	06-Oct-2022	6.5	Those using JXPath to interpret XPath may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40158**	N/A	A-APA-COMM-201022/6
Out-of-bounds Write	06-Oct-2022	6.5	Those using JXPath to interpret XPath may be vulnerable to Denial of Service attacks (DOS). If the parser is running	N/A	A-APA-COMM-201022/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40159**		
Out-of-bounds Write	06-Oct-2022	6.5	Those using JXPath to interpret XPath may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40160**	N/A	A-APA-COMM-201022/8
Out-of-bounds Write	06-Oct-2022	6.5	Those using JXPath to interpret XPath may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support	N/A	A-APA-COMM-201022/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service attack. **CVE ID : CVE-2022-40161**		
Product: shiro					
Affected Version(s): * Up to (excluding) 1.10.0					
Improper Authentication	12-Oct-2022	9.8	Apache Shiro before 1.10.0, Authentication Bypass Vulnerability in Shiro when forwarding or including via RequestDispatcher. **CVE ID : CVE-2022-40664**	https://lists.apache.org/thread/loc2ktxng32xpy7lfwxto13k4lvnhjwg	A-APA-SHIR-201022/10
Vendor: Autodesk					
Product: advanced_material_exchange					
Affected Version(s): 2019					
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted file consumed through Moldflow Synergy, Moldflow Adviser, Moldflow Communicator, and Advanced Material Exchange applications could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0019	A-AUT-ADVA-201022/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33883		
Affected Version(s): 2021					
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted file consumed through Moldflow Synergy, Moldflow Adviser, Moldflow Communicator, and Advanced Material Exchange applications could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33883**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0019	A-AUT-ADVA-201022/12
Product: autocad					
Affected Version(s): * Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33889		
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/14
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/16
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/17
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/19
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	k-sa-2022-0020	
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/21
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/23
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**		
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/25
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-33884**		
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/27
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: autocad_advance_steel					
Affected Version(s): * Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/29
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/30
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/31
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/32
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	k-sa-2022-0020	
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/34
Improper Handling of Exceptiona	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	k-sa-2022-0020	
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/36
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**		
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/38
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/40
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-33888**		
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/42
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/44
Product: autocad_architecture					
Affected Version(s): * Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/45
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed	https://www.autodesk.com/trust/security-	A-AUT-AUTO-201022/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	advisories/adsk-sa-2022-0021	
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/47
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	k-sa-2022-0020	
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/49
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/51
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**		
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/53
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33885		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/55
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2022-33887**		
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/57
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/59
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/60
Product: autocad_civil_3d					
Affected Version(s): * Up to (excluding) 2022.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/61
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/62
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	k-sa-2022-0020	
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/64
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/66
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**		
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/68
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-33884**		
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/70
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code. **CVE ID : CVE-2022-33886**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/72
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33888		
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/74
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/75
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	k-sa-2022-0021	
Product: autocad_electrical					
Affected Version(s): * Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/77
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**		
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/79
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**		
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/81
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/83
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the context of the current process. **CVE ID : CVE-2022-33888**		
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/85
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/86
Improper Handling of	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be	https://www.autodesk.com/trust/security-	A-AUT-AUTO-201022/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	advisories/adsk-sa-2022-0020	
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/89
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/90
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed	https://www.autodesk.com/trust/security-	A-AUT-AUTO-201022/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	advisories/adsk-sa-2022-0021	
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/92
Product: autocad_lt					
Affected Version(s): * Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**		
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/94
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**		
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/96
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33885		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/98
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2022-33887**		
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/100
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/102
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/104
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/105
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	k-sa-2022-0020	
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/107
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**		
Product: autocad_map_3d					
Affected Version(s): * Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/109
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**		
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/111
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-33884**		
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/113
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code. **CVE ID : CVE-2022-33886**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/115
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33888		
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/117
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/118
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/120
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	k-sa-2022-0020	
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/122
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**		
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/124
Product: autocad_mechanical					
Affected Version(s): * Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**		
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/126
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-33884**		
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/128
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/129
Improper Handling	03-Oct-2022	7.8	A maliciously crafted MODEL and	https://www.autodesk.com/tr	A-AUT-AUTO-201022/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Exceptional Conditions			SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	ust/security-advisories/adsk-sa-2022-0020	
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/132
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/133
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when	https://www.autodesk.com/trust/security-	A-AUT-AUTO-201022/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	advisories/adsk-sa-2022-0020	
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/135
Improper Handling of Exceptiona	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	k-sa-2022-0020	
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/137
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**		
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/139
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the context of the current process. **CVE ID : CVE-2022-33890**		
Product: autocad_mep					
Affected Version(s): * Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/141
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33890		
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/143
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/144
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/145
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/147
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/148
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	k-sa-2022-0020	
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/150
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/152
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**		
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/154
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2022-33889**		
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/156
Product: autocad_plant_3d					
Affected Version(s): * Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33889		
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/158
Affected Version(s): From (including) 2020 Up to (excluding) 2020.1.6					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2021 Up to (excluding) 2021.1.3					
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/160
Affected Version(s): From (including) 2022 Up to (excluding) 2022.1.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/161
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/163
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-201022/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	k-sa-2022-0020	
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33884**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/165
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted X_B, CATIA, and PDF file when parsed through Autodesk AutoCAD 2023 and 2022 can be used to write beyond the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-33885**		
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted MODEL and SLDPRT file can be used to write beyond the allocated buffer while parsing through Autodesk AutoCAD 2023 and 2022. The vulnerability exists because the application fails to handle crafted MODEL and SLDPRT files, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2022-33886**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/167
Improper Handling of Exceptional Conditions	03-Oct-2022	7.8	A maliciously crafted PDF file when parsed through Autodesk AutoCAD 2023 causes an unhandled exception. An attacker can leverage this	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to cause a crash or read sensitive data or execute arbitrary code in the context of the current process. **CVE ID : CVE-2022-33887**		
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted Dwg2Spd file when processed through Autodesk DWG application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33888**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/169
Out-of-bounds Read	03-Oct-2022	7.5	Parsing a maliciously crafted X_B file can force Autodesk AutoCAD 2023 and 2022 to read beyond allocated boundaries. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-AUTO-201022/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-33884**		
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/171
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-AUTO-201022/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: autodesk_desktop					
Affected Version(s): * Up to (including) 8.4.0.50					
N/A	03-Oct-2022	9.8	Under certain conditions, an attacker could create an unintended sphere of control through a vulnerability present in file delete operation in Autodesk desktop app (ADA). An attacker could leverage this vulnerability to escalate privileges and execute arbitrary code. **CVE ID : CVE-2022-33882**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0015	A-AUT-AUTO-201022/173
Product: design_review					
Affected Version(s): * Up to (excluding) 2018					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-DESI-201022/174
Affected Version(s): 2018					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted GIF or JPEG files when parsed through Autodesk Design Review 2018, and AutoCAD 2023 and 2022 could be used to write beyond the allocated heap buffer. This vulnerability could lead to arbitrary code execution. **CVE ID : CVE-2022-33889**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-DESI-201022/175
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PCT or DWF file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33890**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0021	A-AUT-DESI-201022/176
Product: moldflow_adviser					
Affected Version(s): 2019					
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted file consumed through Moldflow	https://www.autodesk.com/trust/security-	A-AUT-MOLD-201022/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Synergy, Moldflow Adviser, Moldflow Communicator, and Advanced Material Exchange applications could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33883**	advisories/adsk-sa-2022-0019	
Affected Version(s): 2021					
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted file consumed through Moldflow Synergy, Moldflow Adviser, Moldflow Communicator, and Advanced Material Exchange applications could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33883**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0019	A-AUT-MOLD-201022/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: moldflow_communicator					
Affected Version(s): 2019					
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted file consumed through Moldflow Synergy, Moldflow Adviser, Moldflow Communicator, and Advanced Material Exchange applications could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33883**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0019	A-AUT-MOLD-201022/179
Affected Version(s): 2021					
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted file consumed through Moldflow Synergy, Moldflow Adviser, Moldflow Communicator, and Advanced Material Exchange applications could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0019	A-AUT-MOLD-201022/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the context of the current process. **CVE ID : CVE-2022-33883**		
Product: moldflow_synergy					
Affected Version(s): 2019					
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted file consumed through Moldflow Synergy, Moldflow Adviser, Moldflow Communicator, and Advanced Material Exchange applications could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33883**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0019	A-AUT-MOLD-201022/181
Affected Version(s): 2021					
Out-of-bounds Write	03-Oct-2022	7.8	A malicious crafted file consumed through Moldflow Synergy, Moldflow Adviser, Moldflow Communicator, and Advanced Material Exchange applications could lead to memory corruption vulnerability. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0019	A-AUT-MOLD-201022/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-33883**		
Product: subassembly_composer					
Affected Version(s): From (including) 2020 Up to (excluding) 2020.6.3					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PKT file when consumed through SubassemblyComposer.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41301**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0018	A-AUT-SUBA-201022/183
Affected Version(s): From (including) 2021 Up to (excluding) 2021.3.2					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PKT file when consumed through SubassemblyComposer.exe application could lead to memory corruption	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0018	A-AUT-SUBA-201022/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41301**		
Affected Version(s): From (including) 2022 Up to (excluding) 2022.2.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PKT file when consumed through SubassemblyComposer.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41301**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0018	A-AUT-SUBA-201022/185
Affected Version(s): From (including) 2023 Up to (excluding) 2023.1					
Out-of-bounds Write	03-Oct-2022	7.8	A maliciously crafted PKT file when consumed through SubassemblyComposer.exe application	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0018	A-AUT-SUBA-201022/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-41301**		
Vendor: Avaya					
Product: aura_application_enablement_services					
Affected Version(s): From (including) 10.1.0.0 Up to (excluding) 10.1.0.2					
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	6.7	A vulnerability related to weak permissions was detected in Avaya Aura Application Enablement Services web application, allowing an administrative user to modify accounts leading to execution of arbitrary code as the root user. This issue affects Application Enablement Services versions 8.0.0.0 through 8.1.3.4 and 10.1.0.0 through 10.1.0.1. Versions prior to 8.0.0.0 are end of	https://download.avaya.com/css/public/documents/101083688	A-AVA-AURA-201022/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manufacturing support and were not evaluated. **CVE ID : CVE-2022-2975**		
Affected Version(s): From (including) 8.0.0.0 Up to (excluding) 8.1.3.5					
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	6.7	A vulnerability related to weak permissions was detected in Avaya Aura Application Enablement Services web application, allowing an administrative user to modify accounts leading to execution of arbitrary code as the root user. This issue affects Application Enablement Services versions 8.0.0.0 through 8.1.3.4 and 10.1.0.0 through 10.1.0.1. Versions prior to 8.0.0.0 are end of manufacturing support and were not evaluated. **CVE ID : CVE-2022-2975**	https://download.avaya.com/css/public/documents/101083688	A-AVA-AURA-201022/188
Product: aura_communication_manager					
Affected Version(s): 10.1.0.0					
Improper Privilege Management	12-Oct-2022	6.7	Privilege escalation related vulnerabilities were discovered in Avaya Aura	https://download.avaya.com/css/public/docu	A-AVA-AURA-201022/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Communication Manager that may allow local administrative users to escalate their privileges. This issue affects Communication Manager versions 8.0.0.0 through 8.1.3.3 and 10.1.0.0. **CVE ID : CVE-2022-2249**	ments/101083760	
Affected Version(s): From (including) 8.0 Up to (excluding) 8.1.3.4					
Improper Privilege Management	12-Oct-2022	6.7	Privilege escalation related vulnerabilities were discovered in Avaya Aura Communication Manager that may allow local administrative users to escalate their privileges. This issue affects Communication Manager versions 8.0.0.0 through 8.1.3.3 and 10.1.0.0. **CVE ID : CVE-2022-2249**	https://download.avaya.com/css/public/documents/101083760	A-AVA-AURA-201022/190
Vendor: axiosys					
Product: bento4					
Affected Version(s): 1.6.0-639					
Out-of-bounds Write	03-Oct-2022	8.8	Bento4 v1.6.0-639 was discovered to contain a heap overflow via the AP4_BitReader::Rea	N/A	A-AXI-BENT-201022/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dBits function in mp4mux. **CVE ID : CVE-2022-41428**		
Out-of-bounds Write	03-Oct-2022	8.8	Bento4 v1.6.0-639 was discovered to contain a heap overflow via the AP4_Atom::TypeFromString function in mp4tag. **CVE ID : CVE-2022-41429**	https://github.com/axiomatic-systems/Bento4/issues/773	A-AXI-BENT-201022/192
Out-of-bounds Write	03-Oct-2022	8.8	Bento4 v1.6.0-639 was discovered to contain a heap overflow via the AP4_BitReader::ReadBit function in mp4mux. **CVE ID : CVE-2022-41430**	https://github.com/axiomatic-systems/Bento4/issues/773	A-AXI-BENT-201022/193
Missing Release of Memory after Effective Lifetime	03-Oct-2022	6.5	Bento4 v1.6.0-639 was discovered to contain a memory leak via the AP4_Processor::Process function in the mp4encrypt binary. **CVE ID : CVE-2022-41419**	N/A	A-AXI-BENT-201022/194
N/A	03-Oct-2022	6.5	Bento4 v1.6.0-639 was discovered to contain a segmentation violation in the mp4fragment component. **CVE ID : CVE-2022-41423**	N/A	A-AXI-BENT-201022/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	03-Oct-2022	6.5	Bento4 v1.6.0-639 was discovered to contain a memory leak via the AP4_SttsAtom::Create function in mp42hls. **CVE ID : CVE-2022-41424**	N/A	A-AXI-BENT-201022/196
N/A	03-Oct-2022	6.5	Bento4 v1.6.0-639 was discovered to contain a segmentation violation via the AP4_Processor::ProcessFragments function in mp4decrypt. **CVE ID : CVE-2022-41425**	N/A	A-AXI-BENT-201022/197
Missing Release of Memory after Effective Lifetime	03-Oct-2022	6.5	Bento4 v1.6.0-639 was discovered to contain a memory leak via the AP4_AtomFactory::CreateAtomFromStream function in mp4split. **CVE ID : CVE-2022-41426**	N/A	A-AXI-BENT-201022/198
Missing Release of Memory after Effective Lifetime	03-Oct-2022	6.5	Bento4 v1.6.0-639 was discovered to contain a memory leak in the AP4_AvcFrameParser::Feed function in mp4mux. **CVE ID : CVE-2022-41427**	N/A	A-AXI-BENT-201022/199
Vendor: backdropcms					
Product: backdrop_cms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.22.0					
Unrestricted Upload of File with Dangerous Type	07-Oct-2022	7.2	Backdrop CMS 1.22.0 has Unrestricted File Upload vulnerability via 'themes' that allows attackers to Remote Code Execution. **CVE ID : CVE-2022-42092**	N/A	A-BAC-BACK-201022/200
Vendor: beckmancoulter					
Product: remisol_advance					
Affected Version(s): * Up to (including) 2.0.12.1					
Incorrect Default Permissions	06-Oct-2022	7.8	A vulnerability was discovered in the Remisol Advance v2.0.12.1 and below for the Normand Message Server. On installation, the permissions set by Remisol Advance allow non-privileged users to overwrite and/or manipulate executables and libraries that run as the elevated SYSTEM user on Windows. **CVE ID : CVE-2022-26235**	https://www.beckmancoulter.com/products/clinical-information-management-tools/remisol-advance	A-BEC-REMI-201022/201
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	6.5	The default privileges for the running service Normand Message Buffer in Beckman Coulter Remisol	N/A	A-BEC-REMI-201022/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Advance v2.0.12.1 and prior allows non-privileged users to overwrite and manipulate executables and libraries. This allows attackers to access sensitive data. **CVE ID : CVE-2022-26240**		
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	5.5	The default privileges for the running service Normand Remisol Advance Launcher in Beckman Coulter Remisol Advance v2.0.12.1 and prior allows non-privileged users to overwrite and manipulate executables and libraries. This allows attackers to access sensitive data. **CVE ID : CVE-2022-26236**	N/A	A-BEC-REMI-201022/203
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	5.5	The default privileges for the running service Normand Viewer Service in Beckman Coulter Remisol Advance v2.0.12.1 and prior allows non-privileged users to overwrite and manipulate executables and	N/A	A-BEC-REMI-201022/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			libraries. This allows attackers to access sensitive data. **CVE ID : CVE-2022-26237**		
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	5.5	The default privileges for the running service Normand Service Manager in Beckman Coulter Remisol Advance v2.0.12.1 and prior allows non-privileged users to overwrite and manipulate executables and libraries. This allows attackers to access sensitive data. **CVE ID : CVE-2022-26238**	N/A	A-BEC-REMI-201022/205
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	5.5	The default privileges for the running service Normand License Manager in Beckman Coulter Remisol Advance v2.0.12.1 and prior allows unprivileged users to overwrite and manipulate executables and libraries. This allows attackers to access sensitive data.	N/A	A-BEC-REMI-201022/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26239		
Vendor: Bentley					
Product: microstation					
Affected Version(s): * Up to (excluding) 10.17.01.58					
Out-of-bounds Read	13-Oct-2022	7.8	Bentley MicroStation and MicroStation-based applications may be affected by out-of-bounds read and stack overflow issues when opening crafted SKP files. Exploiting these issues could lead to information disclosure and code execution. The fixed versions are 10.17.01.58* for MicroStation and 10.17.01.19* for Bentley View. **CVE ID : CVE-2022-42899**	https://www.bentley.com/legal/common-vulnerability-exposure-be-2022-0017/	A-BEN-MICR-201022/207
Out-of-bounds Read	13-Oct-2022	7.8	Bentley MicroStation and MicroStation-based applications may be affected by out-of-bounds read issues when opening crafted FBX files. Exploiting these issues could lead to information disclosure and code execution. The fixed versions are 10.17.01.58* for MicroStation and	https://www.bentley.com/legal/common-vulnerability-exposure-be-2022-0019/	A-BEN-MICR-201022/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.17.01.19* for Bentley View. **CVE ID : CVE-2022-42900**		
Out-of-bounds Read	13-Oct-2022	7.8	Bentley MicroStation and MicroStation-based applications may be affected by out-of-bounds and stack overflow issues when opening crafted XMT files. Exploiting these issues could lead to information disclosure and code execution. The fixed versions are 10.17.01.58* for MicroStation and 10.17.01.19* for Bentley View. **CVE ID : CVE-2022-42901**	https://www.bentley.com/legal/common-vulnerability-exposure-be-2022-0018/	A-BEN-MICR-201022/209
Product: view					
Affected Version(s): * Up to (excluding) 10.17.01.19					
Out-of-bounds Read	13-Oct-2022	7.8	Bentley MicroStation and MicroStation-based applications may be affected by out-of-bounds read and stack overflow issues when opening crafted SKP files. Exploiting these issues could lead to information disclosure and code execution. The fixed versions are	https://www.bentley.com/legal/common-vulnerability-exposure-be-2022-0017/	A-BEN-VIEW-201022/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.17.01.58* for MicroStation and 10.17.01.19* for Bentley View. **CVE ID : CVE-2022-42899**		
Out-of-bounds Read	13-Oct-2022	7.8	Bentley MicroStation and MicroStation-based applications may be affected by out-of-bounds read issues when opening crafted FBX files. Exploiting these issues could lead to information disclosure and code execution. The fixed versions are 10.17.01.58* for MicroStation and 10.17.01.19* for Bentley View. **CVE ID : CVE-2022-42900**	https://www.bentley.com/legal/common-vulnerability-exposure-be-2022-0019/	A-BEN-VIEW-201022/211
Out-of-bounds Read	13-Oct-2022	7.8	Bentley MicroStation and MicroStation-based applications may be affected by out-of-bounds and stack overflow issues when opening crafted XMT files. Exploiting these issues could lead to information disclosure and code execution. The fixed versions are 10.17.01.58* for MicroStation and	https://www.bentley.com/legal/common-vulnerability-exposure-be-2022-0018/	A-BEN-VIEW-201022/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.17.01.19* for Bentley View. **CVE ID : CVE-2022-42901**		
Vendor: bevywise					
Product: mqttroute					
Affected Version(s): * Up to (including) 3.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Oct-2022	5.4	A cross-site scripting (XSS) vulnerability in MQTTRoute v3.3 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the dashboard name text field. **CVE ID : CVE-2022-35612**	N/A	A-BEV-MQTT-201022/213
Affected Version(s): 3.3					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	4.3	A Cross-Site Request Forgery (CSRF) in MQTTRoute v3.3 and below allows attackers to create and remove dashboards. **CVE ID : CVE-2022-35611**	N/A	A-BEV-MQTT-201022/214
Vendor: boodskap					
Product: iot_platform					
Affected Version(s): 4.4.9-02					
Improper Authentication	13-Oct-2022	8.8	Boodskap IoT Platform v4.4.9-02 allows attackers to escalate privileges	N/A	A-BOO-IOT_-201022/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted request sent to /api/user/upsert/<uuid>. **CVE ID : CVE-2022-35135**		
Missing Authorization	13-Oct-2022	6.5	Boodskap IoT Platform v4.4.9-02 allows attackers to make unauthenticated API requests. **CVE ID : CVE-2022-35136**	N/A	A-BOO-IOT_-201022/216
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Oct-2022	5.4	Boodskap IoT Platform v4.4.9-02 contains a cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-35134**	N/A	A-BOO-IOT_-201022/217
Vendor: book_store_management_system_project					
Product: book_store_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability was found in SourceCodester Book Store Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /category.php. The manipulation of the argument category_name	N/A	A-BOO-BOOK-201022/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-210436. **CVE ID : CVE-2022-3452**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability was found in SourceCodester Book Store Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /transcation.php. The manipulation of the argument buyer_name leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-210437 was assigned to this vulnerability. **CVE ID : CVE-2022-3453**	N/A	A-BOO-BOOK-201022/219
Vendor: brainvire					
Product: disable_user_login					
Affected Version(s): * Up to (including) 1.0.1					
Cross-Site Request	10-Oct-2022	5.3	The Disable User Login WordPress plugin through 1.0.1 does not have	N/A	A-BRA-DISA-201022/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			authorisation and CSRF checks when updating its settings, allowing unauthenticated attackers to block (or unblock) users at will. **CVE ID : CVE-2022-2350**		
Vendor: browserify-shim_project					
Product: browserify-shim					
Affected Version(s): 3.8.15					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	11-Oct-2022	9.8	Prototype pollution vulnerability in function resolveShims in resolve-shims.js in thlorenz browserify-shim 3.8.15 via the k variable in resolve-shims.js. **CVE ID : CVE-2022-37617**	N/A	A-BRO-BROW-201022/221
Vendor: Centreon					
Product: centreon					
Affected Version(s): 22.04.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-2022	5.4	A cross-site scripting (XSS) vulnerability in Centreon 22.04.0 allows attackers to execute arbitrary web script or HTML via a crafted payload injected into the Service>Templates	N/A	A-CEN-CENT-201022/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service_alias parameter. **CVE ID : CVE-2022-39988**		
Vendor: cert					
Product: vince					
Affected Version(s): * Up to (excluding) 1.50.4					
URL Redirection to Untrusted Site ('Open Redirect')	10-Oct-2022	5.4	An HTML injection vulnerability exists in CERT/CC VINCE software prior to 1.50.4. An authenticated attacker can inject arbitrary HTML via form using the "Product Affected" field. **CVE ID : CVE-2022-40248**	N/A	A-CER-VINC-201022/223
URL Redirection to Untrusted Site ('Open Redirect')	10-Oct-2022	5.4	An HTML injection vulnerability exists in CERT/CC VINCE software prior to 1.50.4. An authenticated attacker can inject arbitrary HTML via a crafted email with HTML content in the Subject field. **CVE ID : CVE-2022-40257**	N/A	A-CER-VINC-201022/224
Vendor: church_management_system_project					
Product: church_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with	12-Oct-2022	7.2	An arbitrary file upload vulnerability in the /admin/admin_pic.	N/A	A-CHU-CHUR-201022/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			php component of Church Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-41406**		
Vendor: Cisco					
Product: sd-wan_vmanage					
Affected Version(s): 20.7					
Missing Authentication for Critical Function	10-Oct-2022	5.3	A vulnerability in authentication mechanism of Cisco Software-Defined Application Visibility and Control (SD-AVC) on Cisco vManage could allow an unauthenticated, remote attacker to access the GUI of Cisco SD-AVC without authentication. This vulnerability exists because the GUI is accessible on self-managed cloud installations or local server installations of Cisco vManage. An attacker could exploit this vulnerability by accessing the exposed GUI of Cisco SD-AVC. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-avc-NddSGB8	A-CIS-SD-W-201022/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to view managed device names, SD-AVC logs, and SD-AVC DNS server IP addresses. **CVE ID : CVE-2022-20830**		
Affected Version(s): From (including) 18.4 Up to (excluding) 20.3.4.1					
Missing Authentication for Critical Function	10-Oct-2022	5.3	A vulnerability in authentication mechanism of Cisco Software-Defined Application Visibility and Control (SD-AVC) on Cisco vManage could allow an unauthenticated, remote attacker to access the GUI of Cisco SD-AVC without authentication. This vulnerability exists because the GUI is accessible on self-managed cloud installations or local server installations of Cisco vManage. An attacker could exploit this vulnerability by accessing the exposed GUI of Cisco SD-AVC. A successful exploit could allow the attacker to view managed device	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-avc-NddSGB8	A-CIS-SD-W-201022/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			names, SD-AVC logs, and SD-AVC DNS server IP addresses. **CVE ID : CVE-2022-20830**		
Affected Version(s): From (including) 20.4 Up to (excluding) 20.6.1					
Missing Authentication for Critical Function	10-Oct-2022	5.3	A vulnerability in authentication mechanism of Cisco Software-Defined Application Visibility and Control (SD-AVC) on Cisco vManage could allow an unauthenticated, remote attacker to access the GUI of Cisco SD-AVC without authentication. This vulnerability exists because the GUI is accessible on self-managed cloud installations or local server installations of Cisco vManage. An attacker could exploit this vulnerability by accessing the exposed GUI of Cisco SD-AVC. A successful exploit could allow the attacker to view managed device names, SD-AVC logs, and SD-AVC	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-avc-NddSGB8	A-CIS-SD-W-201022/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS server IP addresses. **CVE ID : CVE-2022-20830**		
Vendor: clippercms					
Product: clippercms					
Affected Version(s): 1.3.3					
Server-Side Request Forgery (SSRF)	13-Oct-2022	9.8	ClipperCMS 1.3.3 was discovered to contain a Server-Side Request Forgery (SSRF) via the rss_url_news parameter at /manager/index.php. **CVE ID : CVE-2022-41495**	N/A	A-CLI-CLIP-201022/229
Server-Side Request Forgery (SSRF)	13-Oct-2022	9.8	ClipperCMS 1.3.3 was discovered to contain a Server-Side Request Forgery (SSRF) via the pkg_url parameter at /manager/index.php. **CVE ID : CVE-2022-41497**	N/A	A-CLI-CLIP-201022/230
Vendor: Codeigniter					
Product: codeigniter					
Affected Version(s): 3.0					
Improper Neutralization of Special Elements used in an SQL Command	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.ph	N/A	A-COD-CODE-201022/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			p or_where() function. **CVE ID : CVE-2022-40824**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php where_in() function. **CVE ID : CVE-2022-40825**	N/A	A-COD-CODE-201022/232
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_having() function. **CVE ID : CVE-2022-40826**	N/A	A-COD-CODE-201022/233
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php where() function. **CVE ID : CVE-2022-40827**	N/A	A-COD-CODE-201022/234
Improper Neutralizat	07-Oct-2022	9.8	B.C. Institute of Technology	N/A	A-COD-CODE-201022/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_where_not_in() function. **CVE ID : CVE-2022-40828**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_like() function. **CVE ID : CVE-2022-40829**	N/A	A-COD-CODE-201022/236
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php where_not_in() function. **CVE ID : CVE-2022-40830**	N/A	A-COD-CODE-201022/237
Improper Neutralization of Special Elements used in an SQL Command	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\D	N/A	A-COD-CODE-201022/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			B_query_builder.php like() function. **CVE ID : CVE-2022-40831**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php having() function. **CVE ID : CVE-2022-40832**	N/A	A-COD-CODE-201022/239
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_where_in() function. **CVE ID : CVE-2022-40833**	N/A	A-COD-CODE-201022/240
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_not_like() function. **CVE ID : CVE-2022-40834**	N/A	A-COD-CODE-201022/241
Improper Neutralizat	07-Oct-2022	9.8	B.C. Institute of Technology	N/A	A-COD-CODE-201022/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php. **CVE ID : CVE-2022-40835**		
Affected Version(s): From (including) 3.0 Up to (including) 3.1.13					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_where() function. **CVE ID : CVE-2022-40824**	N/A	A-COD-CODE-201022/243
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php where_in() function. **CVE ID : CVE-2022-40825**	N/A	A-COD-CODE-201022/244
Improper Neutralization of Special Elements used in an SQL Command	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.ph	N/A	A-COD-CODE-201022/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			p or_having() function. **CVE ID : CVE-2022-40826**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php where() function. **CVE ID : CVE-2022-40827**	N/A	A-COD-CODE-201022/246
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_where_not_in() function. **CVE ID : CVE-2022-40828**	N/A	A-COD-CODE-201022/247
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_like() function. **CVE ID : CVE-2022-40829**	N/A	A-COD-CODE-201022/248
Improper Neutralizat	07-Oct-2022	9.8	B.C. Institute of Technology	N/A	A-COD-CODE-201022/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php where_not_in() function. **CVE ID : CVE-2022-40830**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php like() function. **CVE ID : CVE-2022-40831**	N/A	A-COD-CODE-201022/250
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php having() function. **CVE ID : CVE-2022-40832**	N/A	A-COD-CODE-201022/251
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_where_in() function.	N/A	A-COD-CODE-201022/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40833		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php or_not_like() function. **CVE ID : CVE-2022-40834**	N/A	A-COD-CODE-201022/253
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	B.C. Institute of Technology CodeIgniter <=3.1.13 is vulnerable to SQL Injection via system\database\DB_query_builder.php. **CVE ID : CVE-2022-40835**	N/A	A-COD-CODE-201022/254
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.7					
Improper Initialization	06-Oct-2022	4.3	CodeIgniter is a PHP full-stack web framework. In versions prior to 4.2.7 setting `$secure` or `$httponly` value to `true` in `Config\Cookie` is not reflected in `set_cookie()` or `Response::setCookie()`. As a result cookie values are erroneously exposed to scripts.	https://github.com/codeigniter4/CodeIgniter4/security/advisories/GHSA-745p-r637-7vvp, https://github.com/codeigniter4/CodeIgniter4/pull/6544	A-COD-CODE-201022/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It should be noted that this vulnerability does not affect session cookies. Users are advised to upgrade to v4.2.7 or later. Users unable to upgrade are advised to manually construct their cookies either by setting the options in code or by constructing Cookie objects. Examples of each workaround are available in the linked GHSA. **CVE ID : CVE-2022-39284**		
Vendor: crealogix					
Product: ebics_server					
Affected Version(s): 7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2022	6.1	A vulnerability was found in Crealogix EBICS 7.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /ebics-server/ebics.aspx. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has	N/A	A-CRE-EBIC-201022/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. Upgrading to version 7.1 is able to address this issue. It is recommended to upgrade the affected component. VDB-210374 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3442**		
Vendor: creativedream_file_uploader_project					
Product: creativedream_file_uploader					
Affected Version(s): 0.3					
Unrestricted Upload of File with Dangerous Type	03-Oct-2022	9.8	Arbitrary file upload vulnerability in php uploader **CVE ID : CVE-2022-40721**	N/A	A-CRE-CREA-201022/257
Vendor: d-bus_project					
Product: d-bus					
Affected Version(s): From (including) 1.12.0 Up to (excluding) 1.12.24					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.5	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash when	https://www.openwall.com/lists/oss-security/2022/10/06/1, https://gitlab.freedesktop.org/dbus/dbus/-/issues/418	A-D-B-D-BU-201022/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving a message with certain invalid type signatures. **CVE ID : CVE-2022-42010**		
Improper Validation of Array Index	10-Oct-2022	6.5	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash when receiving a message where an array length is inconsistent with the size of the element type. **CVE ID : CVE-2022-42011**	https://www.openwall.com/lists/oss-security/2022/10/06/1	A-D-B-D-BU-201022/259
N/A	10-Oct-2022	6.5	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash by sending a message with attached file	https://www.openwall.com/lists/oss-security/2022/10/06/1, https://gitlab.freedesktop.org/dbus/dbus/-/issues/417	A-D-B-D-BU-201022/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			descriptors in an unexpected format. **CVE ID : CVE-2022-42012**		
Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.14.4					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.5	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash when receiving a message with certain invalid type signatures. **CVE ID : CVE-2022-42010**	https://www.openwall.com/lists/oss-security/2022/10/06/1, https://gitlab.freedesktop.org/dbus/dbus/-/issues/418	A-D-B-D-BU-201022/261
Improper Validation of Array Index	10-Oct-2022	6.5	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash when receiving a message where an array length is inconsistent with the size of the element type.	https://www.openwall.com/lists/oss-security/2022/10/06/1	A-D-B-D-BU-201022/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42011		
N/A	10-Oct-2022	6.5	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash by sending a message with attached file descriptors in an unexpected format. **CVE ID : CVE-2022-42012**	https://www.openwall.com/lists/oss-security/2022/10/06/1, https://gitlab.freedesktop.org/dbus/dbus/-/issues/417	A-D-B-D-BU-201022/263
Affected Version(s): From (including) 1.15.0 Up to (excluding) 1.15.2					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.5	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash when receiving a message with certain invalid type signatures. **CVE ID : CVE-2022-42010**	https://www.openwall.com/lists/oss-security/2022/10/06/1, https://gitlab.freedesktop.org/dbus/dbus/-/issues/418	A-D-B-D-BU-201022/264
Improper Validation	10-Oct-2022	6.5	An issue was discovered in D-Bus	https://www.openwall.com/li	A-D-B-D-BU-201022/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash when receiving a message where an array length is inconsistent with the size of the element type. **CVE ID : CVE-2022-42011**	sts/oss-security/2022/10/06/1	
N/A	10-Oct-2022	6.5	An issue was discovered in D-Bus before 1.12.24, 1.13.x and 1.14.x before 1.14.4, and 1.15.x before 1.15.2. An authenticated attacker can cause dbus-daemon and other programs that use libdbus to crash by sending a message with attached file descriptors in an unexpected format. **CVE ID : CVE-2022-42012**	https://www.openwall.com/lists/oss-security/2022/10/06/1, https://gitlab.freedesktop.org/dbus/dbus/-/issues/417	A-D-B-D-BU-201022/266
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): 5.7.98					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	03-Oct-2022	7.2	DedeCMS 5.7.98 has a file upload vulnerability in the background. **CVE ID : CVE-2022-40886**	N/A	A-DED-DEDE-201022/267
Affected Version(s): 5.7.99					
Unrestricted Upload of File with Dangerous Type	12-Oct-2022	7.2	DedeCMS V5.7.99 was discovered to contain an arbitrary file upload vulnerability via the component /dede/file_manage_control.php. **CVE ID : CVE-2022-40921**	N/A	A-DED-DEDE-201022/268
Vendor: Dell					
Product: cloud_mobility_for_dell_emc_storage					
Affected Version(s): * Up to (excluding) 1.3.1					
Incorrect Authorization	11-Oct-2022	6.7	Cloud Mobility for Dell Storage versions 1.3.0 and earlier contains an Improper Access Control vulnerability within the Postgres database. A threat actor with root level access to either the vApp or containerized versions of Cloud Mobility may potentially exploit this vulnerability, leading to the modification or deletion of tables	https://www.dell.com/support/kbdoc/en-vc/000203434/dsa-2022-264-cloud-mobility-for-dell-storage-security-update-for-an-insecure-database-vulnerability	A-DEL-CLOU-201022/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are required for many of the core functionalities of Cloud Mobility. Exploitation may lead to the compromise of integrity and availability of the normal functionality of the Cloud Mobility application. **CVE ID : CVE-2022-34434**		
Product: container_storage_modules					
Affected Version(s): From (including) 1.3.0 Up to (excluding) 2.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Oct-2022	8.8	Dell Container Storage Modules 1.2 contains an Improper Limitation of a Pathname to a Restricted Directory in goiscsi and gobrick libraries which could lead to OS command injection. A remote unauthenticated attacker could exploit this vulnerability leading to unintentional access to path outside of restricted directory. **CVE ID : CVE-2022-34426**	https://www.dell.com/support/kbdoc/en-vc/000203352/dsa-2022-259-dell-container-storage-modules-security-update-for-multiple-vulnerabilities	A-DEL-CONT-201022/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8.8	Dell Container Storage Modules 1.2 contains an OS Command Injection in goiscsi and gobrick libraries. A remote unauthenticated attacker could exploit this vulnerability leading to modification of intended OS command execution. **CVE ID : CVE-2022-34427**	https://www.dell.com/support/kbdoc/en-vc/000203352/dsa-2022-259-dell-container-storage-modules-security-update-for-multiple-vulnerabilities	A-DEL-CONT-201022/271
Product: geodrive					
Affected Version(s): * Up to (excluding) 2.2.3					
Unquoted Search Path or Element	12-Oct-2022	7.8	Dell GeoDrive, versions prior to 2.2, contains an Unquoted File Path vulnerability. A low privilege attacker could potentially exploit this vulnerability, leading to the execution of arbitrary code in the SYSTEM security context. **CVE ID : CVE-2022-33920**	https://www.dell.com/support/kbdoc/000203632	A-DEL-GEOD-201022/272
Uncontrolled Search Path Element	12-Oct-2022	7.8	Dell GeoDrive, versions prior to 2.2, contains Multiple DLL Hijacking Vulnerabilities. A	https://www.dell.com/support/kbdoc/000203632	A-DEL-GEOD-201022/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			low privilege attacker could potentially exploit this vulnerability, leading to the execution of arbitrary code in the SYSTEM security context. **CVE ID : CVE-2022-33921**		
Incorrect Default Permissions	12-Oct-2022	7.8	Dell GeoDrive, versions prior to 2.2, contains Insecure File and Folder Permissions vulnerabilities. A low privilege attacker could potentially exploit this vulnerability, leading to the execution of arbitrary code in the SYSTEM security context. Dell recommends customers to upgrade at the earliest opportunity. **CVE ID : CVE-2022-33922**	https://www.dell.com/support/kbdoc/000203632	A-DEL-GEOD-201022/274
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Oct-2022	7.1	Dell GeoDrive, Versions 1.0 - 2.2, contain a Path Traversal Vulnerability in the reporting function. A local, low privileged attacker could potentially exploit this	https://www.dell.com/support/kbdoc/000203632	A-DEL-GEOD-201022/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, to gain unauthorized delete access to the files stored on the server filesystem, with the privileges of the GeoDrive service: NT AUTHORITY\SYSTEM. **CVE ID : CVE-2022-33937**		
Affected Version(s): From (including) 2.1.0 Up to (excluding) 2.2.3					
N/A	12-Oct-2022	7.8	Dell GeoDrive, versions 2.1 - 2.2, contains an information disclosure vulnerability in GUI. An authenticated non-admin user could potentially exploit this vulnerability and view sensitive information. **CVE ID : CVE-2022-33919**	https://www.dell.com/support/kbdoc/000203632	A-DEL-GEOD-201022/276
Cleartext Storage of Sensitive Information	12-Oct-2022	5.5	Dell GeoDrive, Versions 2.1 - 2.2, contains an information disclosure vulnerability. An authenticated non-admin user could potentially exploit this vulnerability and gain access to sensitive information.	https://www.dell.com/support/kbdoc/000203632	A-DEL-GEOD-201022/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33918		
Product: hybrid_client					
Affected Version(s): From (including) 1.5 Up to (excluding) 1.8					
N/A	11-Oct-2022	8.2	Dell Hybrid Client below 1.8 version contains a gedit vulnerability. A guest attacker could potentially exploit this vulnerability, allowing deletion of user and some system files and folders. **CVE ID : CVE-2022-34432**	https://www.dell.com/support/kbdoc/en-us/000203345/dsa-2022-260-dell-hybrid-client-security-update-for-multiple-vulnerabilities	A-DEL-HYBR-201022/278
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	11-Oct-2022	7.5	Dell Hybrid Client below 1.8 version contains a Zip Bomb Vulnerability in UI. A guest privilege attacker could potentially exploit this vulnerability, leading to system files modification. **CVE ID : CVE-2022-34430**	https://www.dell.com/support/kbdoc/en-us/000203345/dsa-2022-260-dell-hybrid-client-security-update-for-multiple-vulnerabilities	A-DEL-HYBR-201022/279
N/A	11-Oct-2022	6.5	Dell Hybrid Client below 1.8 version contains a guest user profile corruption vulnerability. A WMS privilege attacker could potentially exploit this vulnerability, leading to DHC	https://www.dell.com/support/kbdoc/en-us/000203345/dsa-2022-260-dell-hybrid-client-security-update-for-multiple-vulnerabilities	A-DEL-HYBR-201022/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system not being accessible. **CVE ID : CVE-2022-34431**		
Product: xtremio_management_server					
Affected Version(s): * Up to (excluding) 6.4.0-22					
Improper Restriction of Excessive Authentication Attempts	12-Oct-2022	9.8	Dell EMC XtremIO versions prior to X2 6.4.0-22 contain a bruteforce vulnerability. A remote unauthenticated attacker can potentially exploit this vulnerability and gain access to an admin account. **CVE ID : CVE-2022-31228**	https://www.dell.com/support/kbdoc/en-us/000204112/dsa-2022-145-dell-emc-xtremeio-for-ssh-and-web-ui-vulnerability	A-DEL-XTRE-201022/281
Vendor: democritus					
Product: d8s-algorithms					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-algorithms package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-dicts package. The affected version is 0.1.0. **CVE ID : CVE-2022-42040**	N/A	A-DEM-D8S--201022/282
Product: d8s-archives					
Affected Version(s): 0.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-archives package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-file-system package. The affected version is 0.1.0. **CVE ID : CVE-2022-41383**	N/A	A-DEM-D8S--201022/283
Product: d8s-asns					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-asns package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-csv package. The affected version is 0.1.0. **CVE ID : CVE-2022-42037**	N/A	A-DEM-D8S--201022/284
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-asns package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-html	N/A	A-DEM-D8S--201022/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			package. The affected version is 0.1.0. **CVE ID : CVE-2022-42044**		
Product: d8s-domains					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-domains package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-urls package. The affected version is 0.1.0. **CVE ID : CVE-2022-41384**	N/A	A-DEM-D8S--201022/286
Product: d8s-file-system					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-file-system package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-hashes package. The affected version is 0.1.0. **CVE ID : CVE-2022-42041**	N/A	A-DEM-D8S--201022/287
Product: d8s-html					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-html package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-urls package. The affected version is 0.1.0. **CVE ID : CVE-2022-41385**	N/A	A-DEM-D8S--201022/288
Product: d8s-ip-addresses					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-ip-addresses package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-csv package. The affected version is 0.1.0. **CVE ID : CVE-2022-42038**	N/A	A-DEM-D8S--201022/289
Product: d8s-json					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-json package for Python, as distributed on PyPI, included a potential code-execution backdoor	N/A	A-DEM-D8S--201022/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inserted by a third party. The backdoor is the democritus-file-system package. The affected version is 0.1.0. **CVE ID : CVE-2022-41382**		
Product: d8s-lists					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-lists package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-dicts package. The affected version is 0.1.0. **CVE ID : CVE-2022-42039**	N/A	A-DEM-D8S--201022/291
Product: d8s-networking					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-networking package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-hashes package. The	N/A	A-DEM-D8S--201022/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected version is 0.1.0. **CVE ID : CVE-2022-42042**		
Product: d8s-pdfs					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-pdfs package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-urls package. The affected version is 0.1.0. **CVE ID : CVE-2022-41387**	N/A	A-DEM-D8S--201022/293
Product: d8s-urls					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-urls package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-csv package. The affected version is 0.1.0. **CVE ID : CVE-2022-42036**	N/A	A-DEM-D8S--201022/294
Product: d8s-utility					
Affected Version(s): 0.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-utility package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-file-system package. The affected version is 0.1.0. **CVE ID : CVE-2022-41381**	N/A	A-DEM-D8S--201022/295
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-utility package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-urls package. The affected version is 0.1.0. **CVE ID : CVE-2022-41386**	N/A	A-DEM-D8S--201022/296
Product: d8s-xml					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-xml package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-html	N/A	A-DEM-D8S--201022/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			package. The affected version is 0.1.0. **CVE ID : CVE-2022-42043**		
Product: d8s-yaml					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	9.8	The d8s-yaml package for Python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-file-system package. The affected version is 0.1.0. **CVE ID : CVE-2022-41380**	N/A	A-DEM-D8S--201022/298
Vendor: discourse					
Product: discotoc					
Affected Version(s): * Up to (excluding) 2.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-2022	5.4	DiscoTOC is a Discourse theme component that generates a table of contents for topics. Users that can create topics in TOC-enabled categories (and have sufficient trust level - configured in component's settings) are able to inject arbitrary HTML on that topic's page. The	https://github.com/discourse/DiscoTOC/commit/f80c215a283cd045d2a371403e6eba88b2911192, https://github.com/discourse/DiscoTOC/security/advisories/GHSA-m44p-w923-w32h	A-DIS-DISC-201022/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue has been fixed on the `main` branch. Admins can update the theme component through the admin UI (Customize -> Themes -> Components -> DiscoTOC -> Check for Updates). Alternatively, admins can temporarily disable the DiscoTOC theme component. **CVE ID : CVE-2022-39270**		
Product: discourse-chat					
Affected Version(s): * Up to (excluding) 0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-2022	5.4	discourse-chat is a plugin for the Discourse message board which adds chat functionality. In versions prior to 0.9 some places render a chat channel's name and description in an unsafe way, allowing staff members to cause an cross site scripting (XSS) attack by inserting unsafe HTML into them. Version 0.9 has addressed this issue. Users are advised to upgrade. There are no known	https://github.com/discourse/discourse-chat/security/advisories/GHSA-qp62-8m3c-9jgj, https://github.com/discourse/discourse-chat/commit/25737733af48e5b9fa60b0561d7fde14bea13cce	A-DIS-DISC-201022/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-39279**		
Vendor: django-mfa2_project					
Product: django-mfa2					
Affected Version(s): * Up to (excluding) 2.5.1					
Authentication Bypass by Capture-replay	11-Oct-2022	7.5	mfa/FIDO2.py in django-mfa2 before 2.5.1 and 2.6.x before 2.6.1 allows a replay attack that could be used to register another device for a user. The device registration challenge is not invalidated after usage. **CVE ID : CVE-2022-42731**	N/A	A-DJA-DJAN-201022/301
Affected Version(s): From (including) 2.6.0 Up to (excluding) 2.6.1					
Authentication Bypass by Capture-replay	11-Oct-2022	7.5	mfa/FIDO2.py in django-mfa2 before 2.5.1 and 2.6.x before 2.6.1 allows a replay attack that could be used to register another device for a user. The device registration challenge is not invalidated after usage. **CVE ID : CVE-2022-42731**	N/A	A-DJA-DJAN-201022/302
Vendor: Dolibarr					
Product: dolibarr_erp\/crm					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 15.0.3					
Incorrect Default Permissions	12-Oct-2022	9.8	Dolibarr ERP & CRM <=15.0.3 is vulnerable to Eval injection. By default, any administrator can be added to the installation page of dolibarr, and if successfully added, malicious code can be inserted into the database and then execute it by eval. **CVE ID : CVE-2022-40871**	N/A	A-DOL-DOLI-201022/303
Vendor: donation_thermometer_project					
Product: donation_thermometer					
Affected Version(s): * Up to (excluding) 2.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2022	4.8	The Donation Thermometer WordPress plugin before 2.1.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-3128**	N/A	A-DON-DONA-201022/304
Vendor: dsgvo-for-wp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dsgvo_all_in_one_for_wp					
Affected Version(s): * Up to (excluding) 4.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2022	4.8	The DSGVO All in one for WP WordPress plugin before 4.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2628**	N/A	A-DSG-DSGV-201022/305
Vendor: F-secure					
Product: atlant					
Affected Version(s): -					
N/A	12-Oct-2022	7.5	Multiple Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aerdl.dll unpacker handler function crashes. This can lead to a possible scanning engine crash. **CVE ID : CVE-2022-28887**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-ATLA-201022/306
Product: elements_endpoint_detection_and_response					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	12-Oct-2022	7.5	Multiple Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aerdl.dll unpacker handler function crashes. This can lead to a possible scanning engine crash. **CVE ID : CVE-2022-28887**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-ELEM-201022/307
Product: elements_endpoint_protection					
Affected Version(s): -					
N/A	12-Oct-2022	7.5	Multiple Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aerdl.dll unpacker handler function crashes. This can lead to a possible scanning engine crash. **CVE ID : CVE-2022-28887**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-ELEM-201022/308
Product: internet_gatekeeper					
Affected Version(s): -					
N/A	12-Oct-2022	7.5	Multiple Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure	https://www.f-secure.com/en/business/support-and-downloads/security-	A-F-S-INTE-201022/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products whereby the aerdl.dll unpacker handler function crashes. This can lead to a possible scanning engine crash. **CVE ID : CVE-2022-28887**	advisories, https://www.withsecure.com/en/support/security-advisories	
Product: linux_security					
Affected Version(s): -					
N/A	12-Oct-2022	7.5	Multiple Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aerdl.dll unpacker handler function crashes. This can lead to a possible scanning engine crash. **CVE ID : CVE-2022-28887**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-LINU-201022/310
Product: linux_security_64					
Affected Version(s): -					
N/A	12-Oct-2022	7.5	Multiple Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aerdl.dll unpacker handler function crashes. This can lead to a possible scanning engine crash.	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-LINU-201022/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28887		
Vendor: Facebook					
Product: hermes					
Affected Version(s): * Up to (excluding) 0.12.0					
Out-of-bounds Write	11-Oct-2022	9.8	An out of bounds write in hermes, while handling large arrays, prior to commit 06eaec767e376bfdb883d912cb15e987ddf2bda1 allows attackers to potentially execute arbitrary code via crafted JavaScript. Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2022-32234**	https://github.com/facebook/hermes/commit/06eaec767e376bfdb883d912cb15e987ddf2bda1, https://www.facebook.com/security/advisories/CVE-2022-32234	A-FAC-HERM-201022/312
Integer Overflow or Wraparound	11-Oct-2022	9.8	A write-what-where condition in hermes caused by an integer overflow, prior to commit 5b6255ae049fa4641791e47fad994e8e8c4da374 allows attackers to potentially execute arbitrary code via crafted JavaScript.	https://www.facebook.com/security/advisories/CVE-2022-35289, https://github.com/facebook/hermes/commit/5b6255ae049fa4641791e47fad994e8e8c4da374	A-FAC-HERM-201022/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note that this is only exploitable if the application using Hermes permits evaluation of untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2022-35289**		
Uncontrolled Recursion	06-Oct-2022	7.5	It was possible to trigger an infinite recursion condition in the error handler when Hermes executed specific maliciously formed JavaScript. This condition was only possible to trigger in dev-mode (when asserts were enabled). This issue affects Hermes versions prior to v0.12.0. **CVE ID : CVE-2022-27810**	https://www.facebook.com/security/advisories/cve-2022-27810	A-FAC-HERM-201022/314
Affected Version(s): * Up to (excluding) 2022-09-27					
Incorrect Conversion between Numeric Types	11-Oct-2022	9.8	An integer conversion error in Hermes bytecode generation, prior to commit 6aa825e480d48127b480b08d13adf70033237097, could have been used to perform Out-Of-Bounds operations	https://www.facebook.com/security/advisories/CVE-2022-40138, https://github.com/facebook/hermes/commit/6aa825e480d48127b480b08	A-FAC-HERM-201022/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and subsequently execute arbitrary code. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2022-40138**	d13adf70033237097	
Vendor: Fasterxml					
Product: jackson-databind					
Affected Version(s): * Up to (excluding) 2.13.4					
Deserialization of Untrusted Data	02-Oct-2022	7.5	In FasterXML jackson-databind before 2.13.4, resource exhaustion can occur because of a lack of a check in BeanDeserializer._deserializeFromArray to prevent use of deeply nested arrays. An application is vulnerable only with certain customized choices for deserialization. **CVE ID : CVE-2022-42004**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50490, https://github.com/FasterXML/jackson-databind/commit/063183589218fec19a9293ed2f17ec53ea80ba88,https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50490	A-FAS-JACK-201022/316
Affected Version(s): * Up to (excluding) 2.14.0					
Deserialization of Untrusted Data	02-Oct-2022	7.5	In FasterXML jackson-databind before 2.14.0-rc1, resource exhaustion can	https://github.com/FasterXML/jackson-databind/commit/d78d00ee7	A-FAS-JACK-201022/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occur because of a lack of a check in primitive value deserializers to avoid deep wrapper array nesting, when the UNWRAP_SINGLE_VALUE_ARRAYS feature is enabled. Additional fix version in 2.13.4.1 and 2.12.17.1 **CVE ID : CVE-2022-42003**	b5245b93103fef3187f70543d67ca33, https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=51020,https://github.com/FasterXML/jackson-databind/commit/d78d00ee7b5245b93103fef3187f70543d67ca33	
Vendor: fastify					
Product: fastify					
Affected Version(s): * Up to (excluding) 4.8.1					
Improper Check for Unusual or Exceptional Conditions	10-Oct-2022	7.5	fastify is a fast and low overhead web framework, for Node.js. Affected versions of fastify are subject to a denial of service via malicious use of the Content-Type header. An attacker can send an invalid Content-Type header that can cause the application to crash. This issue has been addressed in commit `fbb07e8d` and will be included in release version 4.8.1. Users are advised to upgrade. Users unable to	https://github.com/fastify/fastify/security/advisories/GHSA-455w-c45v-86rg, https://github.com/fastify/fastify/commit/fbb07e8dfad74c69cd4cd2211aedab87194618e3	A-FAS-FAST-201022/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade may manually filter out http content with malicious Content-Type headers. **CVE ID : CVE-2022-39288**		
Vendor: Fatfreecrm					
Product: fatfreecrm					
Affected Version(s): * Up to (excluding) 0.20.1					
N/A	08-Oct-2022	6.5	fat_free_crm is a an open source, Ruby on Rails customer relationship management platform (CRM). In versions prior to 0.20.1 an authenticated user can perform a remote Denial of Service attack against Fat Free CRM via bucket access. The vulnerability has been patched in commit `c85a254` and will be available in release `0.20.1`. Users are advised to upgrade or to manually apply patch `c85a254`. There are no known workarounds for this issue. **CVE ID : CVE-2022-39281**	https://github.com/fatfreecrm/fat_free_crm/commit/c85a2546348c2692d32f952c753f7f0b43d1ca71, https://github.com/fatfreecrm/fat_free_crm/security/advisories/GHSA-p75c-5x3h-cxcg	A-FAT-FATF-201022/319
Vendor: Flatpress					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: flatpress					
Affected Version(s): 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	Flatpress v1.2.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the page parameter at /flatpress/admin.php. **CVE ID : CVE-2022-40047**	http://flatpress.com	A-FLA-FLAT-201022/320
Vendor: flyte					
Product: flyteadmin					
Affected Version(s): * Up to (excluding) 1.1.44					
Use of Hard-coded Credentials	06-Oct-2022	7.5	FlyteAdmin is the control plane for the data processing platform Flyte. Users who enable the default Flyte's authorization server without changing the default clientid hashes will be exposed to the public internet. In an effort to make enabling authentication easier for Flyte administrators, the default configuration for Flyte Admin allows access for Flyte Propeller even after turning on authentication via a hardcoded hashed	https://github.com/flyteorg/flyteadmin/pull/478, https://github.com/flyteorg/flyteadmin/security/advisories/GHSA-67x4-qr35-qvrm, https://docs.flyte.org/en/latest/deployment/cluster_config/auth_setup.html#oauth2-authorization-server	A-FLY-FLYT-201022/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password. This password is also set on the default Flyte Propeller configmap in the various Flyte Helm charts. Users who enable auth but do not override this setting in Flyte Admin's configuration may unbeknownst to them be allowing public traffic in by way of this default password with attackers effectively impersonating propeller. This only applies to users who have not specified the ExternalAuthorizationServer setting. Usage of an external auth server automatically turns off this default configuration and are not susceptible to this vulnerability. This issue has been addressed in version 1.1.44. Users should manually set the staticClients in the selfAuthServer section of their configuration if		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they intend to rely on Admin's internal auth server. Again, users who use an external auth server are automatically protected from this vulnerability. **CVE ID : CVE-2022-39273**		
Vendor: fontmeister_project					
Product: fontmeister					
Affected Version(s): * Up to (including) 1.08					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	Reflected Cross-Site Scripting (XSS) vulnerability FontMeister plugin <= 1.08 at WordPress. **CVE ID : CVE-2022-33978**	https://patchstack.com/database/vulnerability/fontmeister/wordpress-fontmeister-plugin-1-08-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve, https://wordpress.org/plugins/fontmeister/	A-FON-FONT-201022/322
Vendor: Fortinet					
Product: fortianalyzer					
Affected Version(s): From (excluding) 5.6.0 Up to (including) 5.6.11					
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8,	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**		
Affected Version(s): From (excluding) 6.0.0 Up to (including) 6.0.11					
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/324
Affected Version(s): From (excluding) 6.2.0 Up to (including) 6.2.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/325
Affected Version(s): From (excluding) 6.4.0 Up to (including) 6.4.8					
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**		
Affected Version(s): From (excluding) 7.0.0 Up to (including) 7.0.3					
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/327
Product: fortimanager					
Affected Version(s): From (excluding) 5.6.0 Up to (including) 5.6.11					
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8,	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**		
Affected Version(s): From (excluding) 6.0.0 Up to (including) 6.0.11					
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/329
Affected Version(s): From (excluding) 6.2.0 Up to (including) 6.2.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/330
Affected Version(s): From (excluding) 6.4.0 Up to (including) 6.4.8					
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**		
Affected Version(s): From (excluding) 7.0.0 Up to (including) 7.0.3					
Exposure of Resource to Wrong Sphere	10-Oct-2022	5.3	An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template images via referencing the name in the URL path. **CVE ID : CVE-2022-26121**	https://fortiguard.com/psirt/FG-IR-22-026	A-FOR-FORT-201022/332
Vendor: freerdp					
Product: freerdp					
Affected Version(s): * Up to (excluding) 2.8.1					
Use of Uninitialized Resource	12-Oct-2022	7.5	FreeRDP is a free remote desktop protocol library and clients. FreeRDP based clients on unix systems using	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-c45q-wcpg-mxjq	A-FRE-FREE-201022/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`/parallel` command line switch might read uninitialized data and send it to the server the client is currently connected to. FreeRDP based server implementations are not affected. Please upgrade to 2.8.1 where this issue is patched. If unable to upgrade, do not use parallel port redirection (`/parallel` command line switch) as a workaround. **CVE ID : CVE-2022-39282**		
Out-of-bounds Read	12-Oct-2022	7.5	FreeRDP is a free remote desktop protocol library and clients. All FreeRDP based clients when using the `/video` command line switch might read uninitialized data, decode it as audio/video and display the result. FreeRDP based server implementations are not affected. This issue has been patched in version	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6cf9-3328-qrvh	A-FRE-FREE-201022/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.8.1. If you cannot upgrade do not use the `/video` switch. **CVE ID : CVE-2022-39283**		
Vendor: getshortcodes					
Product: shortcodes_ultimate					
Affected Version(s): * Up to (including) 5.12.0					
Cross-Site Request Forgery (CSRF)	11-Oct-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Shortcodes Ultimate plugin <= 5.12.0 at WordPress leading to plugin preset settings change. **CVE ID : CVE-2022-38086**	https://patchstack.com/database/vulnerability/shortcodes-ultimate/wordpress-shortcodes-ultimate-plugin-5-12-0-cross-site-request-forgery-csrf-vulnerability?_s_id=cve, https://wordpress.org/plugins/shortcodes-ultimate/#developers	A-GET-SHOR-201022/335
Vendor: gh-pages_project					
Product: gh-pages					
Affected Version(s): 3.1.0					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	12-Oct-2022	9.8	Prototype pollution vulnerability in tschaub gh-pages 3.1.0 via the partial variable in util.js. **CVE ID : CVE-2022-37611**	N/A	A-GH--GH-P-201022/336
Vendor: gin-vue-admin_project					
Product: gin-vue-admin					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Oct-2022	5.4	In "Gin-Vue-Admin", versions v2.5.1 through v2.5.3beta are vulnerable to Unrestricted File Upload that leads to execution of javascript code, through the 'Normal Upload' functionality to the Media Library. When an admin user views the uploaded file, a low privilege attacker will get access to the admin's cookie leading to account takeover. **CVE ID : CVE-2022-32177**	https://github.com/flipped-aurora/gin-vue-admin/blob/v2.5.3beta/web/src/components/upload/common.vue#L29-L37	A-GIN-GIN--201022/337
Affected Version(s): From (including) 2.5.1 Up to (including) 2.5.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Oct-2022	5.4	In "Gin-Vue-Admin", versions v2.5.1 through v2.5.3beta are vulnerable to Unrestricted File Upload that leads to execution of javascript code, through the 'Normal Upload' functionality to the Media Library. When an admin user views the uploaded file, a low privilege attacker will get access to	https://github.com/flipped-aurora/gin-vue-admin/blob/v2.5.3beta/web/src/components/upload/common.vue#L29-L37	A-GIN-GIN--201022/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the admin's cookie leading to account takeover. **CVE ID : CVE-2022-32177**		
Vendor: GNU					
Product: osip					
Affected Version(s): 5.3.0					
Integer Overflow or Wraparound	11-Oct-2022	6.5	GNU oSIP v5.3.0 was discovered to contain an integer overflow via the component osip_body_parse_header. **CVE ID : CVE-2022-41550**	https://savannah.gnu.org/bugs/?63103	A-GNU-OSIP-201022/339
Vendor: Google					
Product: google-protobuf					
Affected Version(s): * Up to (excluding) 3.16.3					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-GOOG-201022/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Affected Version(s): From (including) 3.17.0 Up to (excluding) 3.19.6					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-GOOG-201022/341
Affected Version(s): From (including) 3.20.0 Up to (excluding) 3.20.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-GOOG-201022/342
Affected Version(s): From (including) 3.21.0 Up to (excluding) 3.21.7					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-GOOG-201022/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Product: protobuf-java					
Affected Version(s): * Up to (excluding) 3.16.3					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Affected Version(s): From (including) 3.17.0 Up to (excluding) 3.19.6					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/345
Affected Version(s): From (including) 3.20.0 Up to (excluding) 3.20.3					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core	https://github.com/protocolbuffers/protobuf	A-GOO-PROT-201022/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**	/security/advisories/GHSA-h4h5-3hr4-j3g2	
Affected Version(s): From (including) 3.21.0 Up to (excluding) 3.21.7					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Product: protobuf-javalite					
Affected Version(s): * Up to (excluding) 3.16.3					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions mentioned above. **CVE ID : CVE-2022-3171**		
Affected Version(s): From (including) 3.17.0 Up to (excluding) 3.19.6					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/349
Affected Version(s): From (including) 3.20.0 Up to (excluding) 3.20.3					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Affected Version(s): From (including) 3.21.0 Up to (excluding) 3.21.7					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Product: protobuf-kotlin					
Affected Version(s): * Up to (excluding) 3.16.3					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3171		
Affected Version(s): From (including) 3.17.0 Up to (excluding) 3.19.6					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/353
Affected Version(s): From (including) 3.20.0 Up to (excluding) 3.20.3					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Affected Version(s): From (including) 3.21.0 Up to (excluding) 3.21.7					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms,	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Product: protobuf-kotlin-lite					
Affected Version(s): * Up to (excluding) 3.16.3					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 3.17.0 Up to (excluding) 3.19.6					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/357
Affected Version(s): From (including) 3.20.0 Up to (excluding) 3.20.3					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Affected Version(s): From (including) 3.21.0 Up to (excluding) 3.21.7					
N/A	12-Oct-2022	7.5	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection	https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2	A-GOO-PROT-201022/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pauses. We recommend updating to the versions mentioned above. **CVE ID : CVE-2022-3171**		
Vendor: goolytics_project					
Product: goolytics					
Affected Version(s): * Up to (excluding) 1.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2022	4.8	The Goolytics WordPress plugin before 1.1.2 does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-3132**	N/A	A-GOO-GOOL-201022/360
Vendor: Gradle					
Product: enterprise					
Affected Version(s): From (including) 2020.4 Up to (excluding) 2022.3.2					
Incorrect Authorization	07-Oct-2022	7.5	An access-control vulnerability in Gradle Enterprise 2022.4 through 2022.3.1 allows remote attackers to prevent backups from occurring, and send emails with arbitrary text content to the configured	https://security.gradle.com/advisory/2022-12, https://security.gradle.com	A-GRA-ENTE-201022/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installation-administrator contact address, via HTTP access to an accidentally exposed internal endpoint. This is fixed in 2022.3.2. **CVE ID : CVE-2022-41574**		
Vendor: grafana					
Product: grafana					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 8.5.14					
Improper Verification of Cryptographic Signature	13-Oct-2022	7.8	Grafana is an open source observability and data visualization platform. Versions prior to 9.1.8 and 8.5.14 are vulnerable to a bypass in the plugin signature verification. An attacker can convince a server admin to download and successfully run a malicious plugin even though unsigned plugins are not allowed. Versions 9.1.8 and 8.5.14 contain a patch for this issue. As a workaround, do not install plugins downloaded from untrusted sources. **CVE ID : CVE-2022-31123**	https://github.com/grafana/grafana/security/advisories/GHSA-rhxj-gh46-jvw8	A-GRA-GRAF-201022/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.1.8					
Improper Verification of Cryptographic Signature	13-Oct-2022	7.8	Grafana is an open source observability and data visualization platform. Versions prior to 9.1.8 and 8.5.14 are vulnerable to a bypass in the plugin signature verification. An attacker can convince a server admin to download and successfully run a malicious plugin even though unsigned plugins are not allowed. Versions 9.1.8 and 8.5.14 contain a patch for this issue. As a workaround, do not install plugins downloaded from untrusted sources. **CVE ID : CVE-2022-31123**	https://github.com/grafana/grafana/security/advisories/GHSA-rhxj-gh46-jvw8	A-GRA-GRAF-201022/363
Vendor: grunt-karma_project					
Product: grunt-karma					
Affected Version(s): 4.0.1					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	14-Oct-2022	9.8	Prototype pollution vulnerability in karma-runner grunt-karma 4.0.1 via the key variable in grunt-karma.js. **CVE ID : CVE-2022-37602**	N/A	A-GRU-GRUN-201022/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Hancom					
Product: hancom_office_2020					
Affected Version(s): 11.0.0.5357					
Buffer Underwrite ('Buffer Underflow')	07-Oct-2022	7.8	A buffer underflow vulnerability exists in the way Hword of Hancom Office 2020 version 11.0.0.5357 parses XML-based office files. A specially-crafted malformed file can cause memory corruption by using memory before buffer start, which can lead to code execution. A victim would need to access a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-33896**	N/A	A-HAN-HANC-201022/365
Vendor: hashicorp					
Product: nomad					
Affected Version(s): From (including) 1.0.2 Up to (excluding) 1.2.13					
N/A	12-Oct-2022	6.5	HashiCorp Nomad and Nomad Enterprise 1.0.2 up to 1.2.12, and 1.3.5 jobs submitted with an artifact stanza using invalid S3 or GCS URLs can be used to crash client agents. Fixed in 1.2.13, 1.3.6, and 1.4.0.	https://discuss.hashicorp.com/t/hcsec-2022-22-nomad-panics-on-job-submission-with-bad-artifact-stanza-source-url/45420, https://discuss.hashicorp.com	A-HAS-NOMA-201022/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41606		
Affected Version(s): From (including) 1.3.0 Up to (excluding) 1.3.6					
N/A	12-Oct-2022	6.5	HashiCorp Nomad and Nomad Enterprise 1.0.2 up to 1.2.12, and 1.3.5 jobs submitted with an artifact stanza using invalid S3 or GCS URLs can be used to crash client agents. Fixed in 1.2.13, 1.3.6, and 1.4.0. **CVE ID : CVE-2022-41606**	https://discuss.hashicorp.com/t/hcsec-2022-22-nomad-panics-on-job-submission-with-bad-artifact-stanza-source-url/45420, https://discuss.hashicorp.com	A-HAS-NOMA-201022/367
Product: packer					
Affected Version(s): * Up to (excluding) 2.3.1					
Improper Privilege Management	11-Oct-2022	7.8	An issue was discovered in Hashicorp Packer before 2.3.1. The recommended sudoers configuration for Vagrant on Linux is insecure. If the host has been configured according to this documentation, non-privileged users on the host can leverage a wildcard in the sudoers configuration to execute arbitrary commands as root.	https://discuss.hashicorp.com/t/hcsec-2022-23-vagrant-nfs-sudoers-configuration-allows-for-local-privilege-escalation/45423, https://github.com/hashicorp/vagrant/pull/12910,https://discuss.hashicorp.com/t/hcsec-2022-23-vagrant-nfs-sudoers-configuration-allows-for-local-privilege-	A-HAS-PACK-201022/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42717	escalation/45423	
Product: vault					
Affected Version(s): * Up to (excluding) 1.9.10					
Improper Certificate Validation	12-Oct-2022	5.3	HashiCorp Vault and Vault Enterprise's TLS certificate auth method did not initially load the optionally configured CRL issued by the role's CA into memory on startup, resulting in the revocation list not being checked if the CRL has not yet been retrieved. Fixed in 1.12.0, 1.11.4, 1.10.7, and 1.9.10. **CVE ID : CVE-2022-41316**	https://discuss.hashicorp.com/t/hcsec-2022-24-vaults-tls-cert-auth-method-only-loaded-crl-after-first-request/45483, https://discuss.hashicorp.com	A-HAS-VAUL-201022/369
Affected Version(s): From (including) 1.10.0 Up to (excluding) 1.10.7					
Improper Certificate Validation	12-Oct-2022	5.3	HashiCorp Vault and Vault Enterprise's TLS certificate auth method did not initially load the optionally configured CRL issued by the role's CA into memory on startup, resulting in the revocation list not being checked if the CRL has not yet been retrieved. Fixed in 1.12.0,	https://discuss.hashicorp.com/t/hcsec-2022-24-vaults-tls-cert-auth-method-only-loaded-crl-after-first-request/45483, https://discuss.hashicorp.com	A-HAS-VAUL-201022/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.11.4, 1.10.7, and 1.9.10. **CVE ID : CVE-2022-41316**		
Affected Version(s): From (including) 1.11.0 Up to (excluding) 1.11.4					
Improper Certificate Validation	12-Oct-2022	5.3	HashiCorp Vault and Vault Enterprise's TLS certificate auth method did not initially load the optionally configured CRL issued by the role's CA into memory on startup, resulting in the revocation list not being checked if the CRL has not yet been retrieved. Fixed in 1.12.0, 1.11.4, 1.10.7, and 1.9.10. **CVE ID : CVE-2022-41316**	https://discuss.hashicorp.com/t/hcsec-2022-24-vaults-tls-cert-auth-method-only-loaded-crl-after-first-request/45483, https://discuss.hashicorp.com	A-HAS-VAUL-201022/371
Vendor: haskell					
Product: aeson					
Affected Version(s): * Up to (excluding) 2.0.1.0					
Uncontrolled Resource Consumption	10-Oct-2022	6.5	The aeson library is not safe to use to consume untrusted JSON input. A remote user could abuse this flaw to produce a hash collision in the underlying unordered-containers library by sending specially crafted	https://cs-syd.eu/posts/2021-09-11-json-vulnerability	A-HAS-AESO-201022/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JSON data, resulting in a denial of service. **CVE ID : CVE-2022-3433**		
Vendor: heartex					
Product: label_studio					
Affected Version(s): * Up to (including) 1.5.0					
Server-Side Request Forgery (SSRF)	03-Oct-2022	6.5	A Server Side Request Forgery (SSRF) in the Data Import module in Heartex - Label Studio Community Edition versions 1.5.0 and earlier allows an authenticated user to access arbitrary files on the system. Furthermore, self-registration is enabled by default in these versions of Label Studio enabling a remote attacker to create a new account and then exploit the SSRF. **CVE ID : CVE-2022-36551**	https://github.com/heartexlabs/label-studio/pull/2840	A-HEA-LABE-201022/373
Vendor: Hitachi					
Product: storage_plug-in					
Affected Version(s): 04.8.0					
Improper Privilege Management	06-Oct-2022	8.8	Incorrect Privilege Assignment vulnerability in Hitachi Storage Plug-in for VMware vCenter allows	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hita	A-HIT-STOR-201022/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote authenticated users to cause privilege escalation. This issue affects: Hitachi Storage Plug-in for VMware vCenter 04.8.0. **CVE ID : CVE-2022-2637**	chi-sec-2022-131/index.html	
Vendor: hsqldb					
Product: hypersql_database					
Affected Version(s): * Up to (excluding) 2.7.1					
N/A	06-Oct-2022	9.8	Those using java.sql.Statement or java.sql.PreparedStatement in hsqldb (HyperSQL DataBase) to process untrusted input may be vulnerable to a remote code execution attack. By default it is allowed to call any static method of any Java class in the classpath resulting in code execution. The issue can be prevented by updating to 2.7.1 or by setting the system property "hsqldb.method_class_names" to classes which are allowed to be called. For example, System.setProperty	N/A	A-HSQ-HYPE-201022/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			("hsqldb.method_class_names", "abc") or Java argument -Dhsqldb.method_class_names="abc" can be used. From version 2.7.1 all classes by default are not accessible except those in java.lang.Math and need to be manually enabled. **CVE ID : CVE-2022-41853**		
Vendor: human_resource_management_system_project					
Product: human_resource_management_system					
Affected Version(s): 1.0					
Improper Access Control	12-Oct-2022	9.8	A vulnerability has been found in SourceCodester Human Resource Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /employeeview.php of the component Image File Handler. The manipulation leads to unrestricted upload. The attack can be launched remotely. The associated identifier of this	N/A	A-HUM-HUMA-201022/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-210559. **CVE ID : CVE-2022-3458**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-Oct-2022	8.8	A vulnerability classified as critical was found in SourceCodester Human Resource Management System 1.0. This vulnerability affects unknown code of the component Profile Photo Handler. The manipulation of the argument parameter leads to os command injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-210772. **CVE ID : CVE-2022-3492**	N/A	A-HUM-HUMA-201022/377
N/A	14-Oct-2022	8.8	A vulnerability was found in SourceCodester Human Resource Management System 1.0 and classified as critical. This issue affects some unknown processing of the file employeeadd.php of the component Admin Panel. The manipulation leads	N/A	A-HUM-HUMA-201022/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to improper access controls. The attack may be initiated remotely. The identifier VDB-210785 was assigned to this vulnerability. **CVE ID : CVE-2022-3496**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Oct-2022	5.4	A vulnerability, which was classified as problematic, has been found in SourceCodester Human Resource Management System 1.0. This issue affects some unknown processing of the component Add Employee Handler. The manipulation of the argument First Name/Middle Name/Last Name leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-210773 was assigned to this vulnerability. **CVE ID : CVE-2022-3493**	N/A	A-HUM-HUMA-201022/379
Improper Neutralization of Input During	14-Oct-2022	5.4	A vulnerability was found in SourceCodester Human Resource Management	N/A	A-HUM-HUMA-201022/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			System 1.0. It has been classified as problematic. Affected is an unknown function of the component Master List. The manipulation of the argument city/state/country/ position leads to cross site scripting. It is possible to launch the attack remotely. VDB-210786 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3497**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Oct-2022	5.4	A vulnerability was found in Human Resource Management System 1.0. It has been classified as problematic. This affects an unknown part of the component Leave Handler. The manipulation of the argument Reason leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated	N/A	A-HUM-HUMA-201022/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-210831. **CVE ID : CVE-2022-3502**		
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Oct-2022	6.5	A vulnerability was found in SourceCodester Human Resource Management System. It has been classified as critical. Affected is an unknown function of the file getstatecity.php. The manipulation of the argument sc leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-210714 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3470**	N/A	A-HUM-HUMA-201022/382
Improper Neutralization of Special Elements used in an SQL Command	13-Oct-2022	6.5	A vulnerability classified as critical has been found in SourceCodester Human Resource Management System. This affects an unknown part of the file	N/A	A-HUM-HUMA-201022/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			getstatecity.php. The manipulation of the argument ci leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-210717 was assigned to this vulnerability. **CVE ID : CVE-2022-3473**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Oct-2022	4.9	A vulnerability was found in SourceCodester Human Resource Management System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file city.php. The manipulation of the argument searccity leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-210715.	N/A	A-HUM-HUMA-201022/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3471		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Oct-2022	4.9	A vulnerability was found in SourceCodester Human Resource Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file city.php. The manipulation of the argument cityedit leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210716. **CVE ID : CVE-2022-3472**	N/A	A-HUM-HUMA-201022/385
Vendor: IBM					
Product: cics_tx					
Affected Version(s): 11.1					
Allocation of Resources Without Limits or Throttling	07-Oct-2022	5.5	IBM CICS TX 11.1 could allow a local user to cause a denial of service due to improper load handling. IBM X-Force ID: 229437. **CVE ID : CVE-2022-34308**	https://www.ibm.com/support/pages/node/6826647, https://exchange.xforce.ibmcloud.com/vulnerabilities/229437, https://www.ib	A-IBM-CICS-201022/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m.com/support/pages/node/6826645	
Product: infosphere_information_server					
Affected Version(s): 11.7					
Improper Privilege Management	07-Oct-2022	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information that should only be available to a privileged user. **CVE ID : CVE-2022-36772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/233299, https://www.ibm.com/support/pages/node/6612325	A-IBM-INFO-201022/387
Insufficient Session Expiration	07-Oct-2022	6.5	IBM InfoSphere Information Server 11.7 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 236699. **CVE ID : CVE-2022-41291**	https://exchange.xforce.ibmcloud.com/vulnerabilities/236699, https://www.ibm.com/support/pages/node/6823109	A-IBM-INFO-201022/388
Product: navigator_mobile					
Affected Version(s): 3.4.1.1					
Incorrect Authorization	11-Oct-2022	5.5	IBM Navigator Mobile Android 3.4.1.1 and 3.4.1.2 app could allow a local user to obtain sensitive information due to improper access control. IBM X-Force ID: 233968.	https://www.ibm.com/support/pages/node/6828469, https://exchange.xforce.ibmcloud.com/vulnerabilities/233968	A-IBM-NAVI-201022/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38388		
Affected Version(s): 3.4.1.2					
Incorrect Authorization	11-Oct-2022	5.5	IBM Navigator Mobile Android 3.4.1.1 and 3.4.1.2 app could allow a local user to obtain sensitive information due to improper access control. IBM X-Force ID: 233968. **CVE ID : CVE-2022-38388**	https://www.ibm.com/support/pages/node/6828469, https://exchange.xforce.ibmcloud.com/vulnerabilities/233968	A-IBM-NAVI-201022/390
Product: qradar_security_information_and_event_manager					
Affected Version(s): 7.4.3					
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	IBM QRadar SIEM 7.4 and 7.5 data node rebalancing does not function correctly when using encrypted hosts which could result in information disclosure. IBM X-Force ID: 225889. **CVE ID : CVE-2022-22480**	https://exchange.xforce.ibmcloud.com/vulnerabilities/225889, https://www.ibm.com/support/pages/node/6826695	A-IBM-QRAD-201022/391
Exposure of Resource to Wrong Sphere	07-Oct-2022	5.5	IBM QRadar SIEM 7.4 and 7.5 could disclose sensitive information via a local service to a privileged user. IBM X-Force ID: 227366. **CVE ID : CVE-2022-30613**	https://exchange.xforce.ibmcloud.com/vulnerabilities/227366, https://www.ibm.com/support/pages/node/6826693	A-IBM-QRAD-201022/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 7.5.0					
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	IBM QRadar SIEM 7.4 and 7.5 data node rebalancing does not function correctly when using encrypted hosts which could result in information disclosure. IBM X-Force ID: 225889. **CVE ID : CVE-2022-22480**	https://exchange.xforce.ibmcloud.com/vulnerabilities/225889, https://www.ibm.com/support/pages/node/6826695	A-IBM-QRAD-201022/393
Exposure of Resource to Wrong Sphere	07-Oct-2022	5.5	IBM QRadar SIEM 7.4 and 7.5 could disclose sensitive information via a local service to a privileged user. IBM X-Force ID: 227366. **CVE ID : CVE-2022-30613**	https://exchange.xforce.ibmcloud.com/vulnerabilities/227366, https://www.ibm.com/support/pages/node/6826693	A-IBM-QRAD-201022/394
Affected Version(s): From (including) 7.4.0 Up to (excluding) 7.4.3					
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	IBM QRadar SIEM 7.4 and 7.5 data node rebalancing does not function correctly when using encrypted hosts which could result in information disclosure. IBM X-Force ID: 225889. **CVE ID : CVE-2022-22480**	https://exchange.xforce.ibmcloud.com/vulnerabilities/225889, https://www.ibm.com/support/pages/node/6826695	A-IBM-QRAD-201022/395
Exposure of Resource	07-Oct-2022	5.5	IBM QRadar SIEM 7.4 and 7.5 could disclose sensitive	https://exchange.xforce.ibmcloud.com/vulne	A-IBM-QRAD-201022/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			information via a local service to a privileged user. IBM X-Force ID: 227366. **CVE ID : CVE-2022-30613**	rabilities/227366, https://www.ibm.com/support/pages/node/6826693	
Product: robotic_process_automation					
Affected Version(s): * Up to (excluding) 21.0.1					
Improper Restriction of Rendered UI Layers or Frames	06-Oct-2022	6.1	IBM Robotic Process Automation 21.0.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 227125. **CVE ID : CVE-2022-22503**	https://exchange.xforce.ibmcloud.com/vulnerabilities/227125, https://www.ibm.com/support/pages/node/6825995	A-IBM-ROBO-201022/397
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.3					
Improper Authentication	06-Oct-2022	5.3	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 is vulnerable to man in the middle attacks through manipulation of the client proxy	https://exchange.xforce.ibmcloud.com/vulnerabilities/233575, https://www.ibm.com/support/pages/node/6826013	A-IBM-ROBO-201022/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration. IBM X-Force ID: 233575. **CVE ID : CVE-2022-36774**		
Affected Version(s): From (including) 21.0.0 Up to (including) 21.0.4					
Origin Validation Error	06-Oct-2022	6.5	IBM Robotic Process Automation 21.0.0, 21.0.1, 21.0.2, 21.0.3, and 21.0.4 is vulnerable to cross origin resource sharing using the bot api. IBM X-Force ID: 236807. **CVE ID : CVE-2022-41294**	https://exchange.xforce.ibmcloud.com/vulnerabilities/236807, https://www.ibm.com/support/pages/node/6825985	A-IBM-ROBO-201022/399
Product: robotic_process_automation_as_a_service					
Affected Version(s): * Up to (excluding) 21.0.1					
Improper Restriction of Rendered UI Layers or Frames	06-Oct-2022	6.1	IBM Robotic Process Automation 21.0.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 227125. **CVE ID : CVE-2022-22503**	https://exchange.xforce.ibmcloud.com/vulnerabilities/227125, https://www.ibm.com/support/pages/node/6825995	A-IBM-ROBO-201022/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.3					
Improper Authentication	06-Oct-2022	5.3	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 is vulnerable to man in the middle attacks through manipulation of the client proxy configuration. IBM X-Force ID: 233575. **CVE ID : CVE-2022-36774**	https://exchange.xforce.ibmcloud.com/vulnerabilities/233575, https://www.ibm.com/support/pages/node/6826013	A-IBM-ROBO-201022/401
Product: robotic_process_automation_for_cloud_pak					
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.3					
Improper Authentication	06-Oct-2022	5.3	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 is vulnerable to man in the middle attacks through manipulation of the client proxy configuration. IBM X-Force ID: 233575. **CVE ID : CVE-2022-36774**	https://exchange.xforce.ibmcloud.com/vulnerabilities/233575, https://www.ibm.com/support/pages/node/6826013	A-IBM-ROBO-201022/402
Affected Version(s): From (including) 21.0.1 Up to (excluding) 21.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-2022	6.1	IBM Robotic Process Automation 21.0.1, 21.0.2, and 21.0.3 for Cloud Pak is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI	https://exchange.xforce.ibmcloud.com/vulnerabilities/234291, https://www.ibm.com/support/pages/node/6826011	A-IBM-ROBO-201022/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 234291. **CVE ID : CVE-2022-38709**		
Product: sterling_partner_engagement_manager					
Affected Version(s): 2.0					
Session Fixation	10-Oct-2022	6.5	IBM Sterling Partner Engagement Manager 2.0 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 229704. **CVE ID : CVE-2022-34334**	https://www.ibm.com/support/pages/node/6828097, https://exchange.xforce.ibmcloud.com/vulnerabilities/229704	A-IBM-STER-201022/404
Affected Version(s): 6.1					
Session Fixation	10-Oct-2022	6.5	IBM Sterling Partner Engagement Manager 2.0 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the	https://www.ibm.com/support/pages/node/6828097, https://exchange.xforce.ibmcloud.com/vulnerabilities/229704	A-IBM-STER-201022/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. IBM X-Force ID: 229704. **CVE ID : CVE-2022-34334**		
Product: websphere_automation_for_ibm_cloud_pak_for_watson_aiops					
Affected Version(s): * Up to (excluding) 1.4.3					
Cross-Site Request Forgery (CSRF)	07-Oct-2022	8.8	IBM WebSphere Automation for Cloud Pak for Watson AIOps 1.4.2 is vulnerable to cross-site request forgery, caused by improper cookie attribute setting. IBM X-Force ID: 226449. **CVE ID : CVE-2022-22493**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226449, https://www.ibm.com/support/pages/node/6826727	A-IBM-WEBS-201022/406
Vendor: idreamsoft					
Product: icms					
Affected Version(s): 7.0.16					
Server-Side Request Forgery (SSRF)	13-Oct-2022	9.8	iCMS v7.0.16 was discovered to contain a Server-Side Request Forgery (SSRF) via the url parameter at admincp.php. **CVE ID : CVE-2022-41496**	N/A	A-IDR-ICMS-201022/407
Vendor: ikus-soft					
Product: rdiffweb					
Affected Version(s): * Up to (excluding) 2.4.10					
Improper Limitation of a Pathname to a	06-Oct-2022	7.5	Path Traversal in GitHub repository ikus060/rdiffweb prior to 2.4.10.	https://huntr.dev/bounties/f7d2a6ab-2faf-4719-bdb6-e4e5d6065752,	A-IKU-RDIF-201022/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			**CVE ID : CVE-2022-3389**	https://github.com/ikus060/rdiffweb/commit/323383d1db656f1b1291be529947bd943a6b0e99	
Affected Version(s): * Up to (excluding) 2.5.0					
Allocation of Resources Without Limits or Throttling	14-Oct-2022	9.8	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.5.0. **CVE ID : CVE-2022-3439**	https://github.com/ikus060/rdiffweb/commit/b78ec09f4582e363f6f449df6f987127e126c311, https://huntr.dev/bounties/37b86c45-b240-4626-bd53-b6f02d10e0d7	A-IKU-RDIF-201022/409
Allocation of Resources Without Limits or Throttling	13-Oct-2022	9.8	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.5.0. **CVE ID : CVE-2022-3456**	https://github.com/ikus060/rdiffweb/commit/b78ec09f4582e363f6f449df6f987127e126c311, https://huntr.dev/bounties/b34412ca-50c5-4615-b7e3-5d07d33acfce	A-IKU-RDIF-201022/410
Origin Validation Error	13-Oct-2022	9.8	Origin Validation Error in GitHub repository ikus060/rdiffweb prior to 2.5.0a5. **CVE ID : CVE-2022-3457**	https://github.com/ikus060/rdiffweb/commit/afc1bdfab5161c74012ff2590a6ec49cc0d8fde0, https://huntr.dev/bounties/cfcab02e-d6ad-	A-IKU-RDIF-201022/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				4dcf-b1b0-da90434bc55b	
URL Redirection to Untrusted Site ('Open Redirect')	10-Oct-2022	6.1	Open Redirect in GitHub repository ikus060/rdiffweb prior to 2.5.0a4. **CVE ID : CVE-2022-3438**	https://huntr.dev/bounties/bc5689e4-221a-4200-a8ab-42c659f89f67, https://github.com/ikus060/rdiffweb/commit/4d464b467f14b8eb9103d7f5f0774e49995527c7	A-IKU-RDIF-201022/412
Affected Version(s): * Up to (including) 2.4.10					
Inadequate Encryption Strength	06-Oct-2022	9.8	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.5.0a4. **CVE ID : CVE-2022-3273**	https://github.com/ikus060/rdiffweb/commit/b5e3bb0a98268d18ceead36ab9b2b7eaacd659a8, https://huntr.dev/bounties/a6df4bad-3382-4add-8918-760d885690f6	A-IKU-RDIF-201022/413
Weak Password Requirements	06-Oct-2022	5.3	Weak Password Requirements in GitHub repository ikus060/rdiffweb prior to 2.5.0a4. **CVE ID : CVE-2022-3376**	https://github.com/ikus060/rdiffweb/commit/2ffc2af65c8f8113b06e0b89929c604bcdf844b9, https://huntr.dev/bounties/a9021e93-6d18-4ac1-98ce-550c4697a4ed	A-IKU-RDIF-201022/414
Affected Version(s): 2.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	06-Oct-2022	9.8	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.5.0a4. **CVE ID : CVE-2022-3273**	https://github.com/ikus060/rdiffweb/commit/b5e3bb0a98268d18ceead36ab9b2b7eaacd659a8, https://huntr.dev/bounties/a6df4bad-3382-4add-8918-760d885690f6	A-IKU-RDIF-201022/415
Origin Validation Error	13-Oct-2022	9.8	Origin Validation Error in GitHub repository ikus060/rdiffweb prior to 2.5.0a5. **CVE ID : CVE-2022-3457**	https://github.com/ikus060/rdiffweb/commit/afc1bdfab5161c74012ff2590a6ec49cc0d8fde0, https://huntr.dev/bounties/cfcab02e-d6ad-4dcf-b1b0-da90434bc55b	A-IKU-RDIF-201022/416
URL Redirection to Untrusted Site ('Open Redirect')	10-Oct-2022	6.1	Open Redirect in GitHub repository ikus060/rdiffweb prior to 2.5.0a4. **CVE ID : CVE-2022-3438**	https://huntr.dev/bounties/bc5689e4-221a-4200-a8ab-42c659f89f67, https://github.com/ikus060/rdiffweb/commit/4d464b467f14b8eb9103d7f5f0774e49995527c7	A-IKU-RDIF-201022/417
Weak Password Requirements	06-Oct-2022	5.3	Weak Password Requirements in GitHub repository ikus060/rdiffweb prior to 2.5.0a4.	https://github.com/ikus060/rdiffweb/commit/2ffc2af65c8f8113b06e0b89929c604bcdf844b9,	A-IKU-RDIF-201022/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3376	https://huntr.dev/bounties/a9021e93-6d18-4ac1-98ce-550c4697a4ed	
Vendor: ini4j_project					
Product: ini4j					
Affected Version(s): * Up to (excluding) 0.5.4					
N/A	11-Oct-2022	7.5	An issue in the fetch() method in the BasicProfile class of org.ini4j before v0.5.4 allows attackers to cause a Denial of Service (DoS) via unspecified vectors. **CVE ID : CVE-2022-41404**	N/A	A-INI-INI4-201022/419
Vendor: integration_for_billingo_\&_gravity_forms_project					
Product: integration_for_billingo_\&_gravity_forms					
Affected Version(s): * Up to (excluding) 1.0.4					
Cross-Site Request Forgery (CSRF)	10-Oct-2022	7.1	The Woo Billingo Plus WordPress plugin before 4.4.5.4, Integration for Billingo & Gravity Forms WordPress plugin before 1.0.4, Integration for Szamlazz.hu & Gravity Forms WordPress plugin before 1.2.7 are lacking CSRF checks in various AJAX actions, which could allow attackers to make logged in Shop	N/A	A-INT-INTE-201022/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Managers and above perform unwanted actions, such as deactivate the plugin's license **CVE ID : CVE-2022-3154**		
Vendor: integration_for_szamlazz.hu_\&_gravity_forms_project					
Product: integration_for_szamlazz.hu_\&_gravity_forms					
Affected Version(s): * Up to (excluding) 1.2.7					
Cross-Site Request Forgery (CSRF)	10-Oct-2022	7.1	The Woo Billingo Plus WordPress plugin before 4.4.5.4, Integration for Billingo & Gravity Forms WordPress plugin before 1.0.4, Integration for Szamlazz.hu & Gravity Forms WordPress plugin before 1.2.7 are lacking CSRF checks in various AJAX actions, which could allow attackers to make logged in Shop Managers and above perform unwanted actions, such as deactivate the plugin's license **CVE ID : CVE-2022-3154**	N/A	A-INT-INTE-201022/421
Vendor: Interspire					
Product: email_marketer					
Affected Version(s): * Up to (including) 6.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	8.8	Interspire Email Marketer through 6.5.0 allows arbitrary file upload via a surveys_submit.php "create survey and submit survey" operation, which can cause a .php file to be accessible under a /admin/temp/surveys/ URI. NOTE: this issue exists because of an incomplete fix for CVE-2018-19550. **CVE ID : CVE-2022-40777**	N/A	A-INT-EMAI-201022/422
Vendor: ISC					
Product: dhcp					
Affected Version(s): 4.1-esv					
NULL Pointer Dereference	07-Oct-2022	7.5	In ISC DHCP 4.4.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1, when the function option_code_hash_lookup() is called from add_option(), it increases the option's refcount field. However, there is not a corresponding call to option_dereference() to decrement the refcount field. The function add_option() is only	https://kb.isc.org/docs/cve-2022-2928	A-ISC-DHCP-201022/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used in server responses to lease query packets. Each lease query response calls this function for several options, so eventually, the reference counters could overflow and cause the server to abort. **CVE ID : CVE-2022-2928**		
Allocation of Resources Without Limits or Throttling	07-Oct-2022	6.5	In ISC DHCP 1.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1 a system with access to a DHCP server, sending DHCP packets crafted to include fqdn labels longer than 63 bytes, could eventually cause the server to run out of memory. **CVE ID : CVE-2022-2929**	https://kb.isc.org/docs/cve-2022-2929	A-ISC-DHCP-201022/424
Affected Version(s): From (including) 1.0.0 Up to (excluding) 4.1-esv					
Allocation of Resources Without Limits or Throttling	07-Oct-2022	6.5	In ISC DHCP 1.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1 a system with access to a DHCP server, sending DHCP packets crafted to include fqdn labels longer than 63 bytes, could	https://kb.isc.org/docs/cve-2022-2929	A-ISC-DHCP-201022/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			eventually cause the server to run out of memory. **CVE ID : CVE-2022-2929**		
Affected Version(s): From (including) 4.2.0 Up to (including) 4.4.3					
Allocation of Resources Without Limits or Throttling	07-Oct-2022	6.5	In ISC DHCP 1.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1 a system with access to a DHCP server, sending DHCP packets crafted to include fqdn labels longer than 63 bytes, could eventually cause the server to run out of memory. **CVE ID : CVE-2022-2929**	https://kb.isc.org/docs/cve-2022-2929	A-ISC-DHCP-201022/426
Affected Version(s): From (including) 4.4.0 Up to (including) 4.4.3					
NULL Pointer Dereference	07-Oct-2022	7.5	In ISC DHCP 4.4.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1, when the function option_code_hash_lookup() is called from add_option(), it increases the option's refcount field. However, there is not a corresponding call to option_dereference() to decrement the refcount field. The function add_option() is only	https://kb.isc.org/docs/cve-2022-2928	A-ISC-DHCP-201022/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used in server responses to lease query packets. Each lease query response calls this function for several options, so eventually, the reference counters could overflow and cause the server to abort. **CVE ID : CVE-2022-2928**		
Vendor: jflyfox					
Product: jfinal_cms					
Affected Version(s): 5.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Oct-2022	8.8	JFinal CMS 5.1.0 is vulnerable to SQL Injection. These interfaces do not use the same component, nor do they have filters, but each uses its own SQL concatenation method, resulting in SQL injection. **CVE ID : CVE-2022-37208**	N/A	A-JFL-JFIN-201022/428
Vendor: jgraph					
Product: mxgraph					
Affected Version(s): 4.2.2					
Improper Neutralization of Input During Web Page Generation	12-Oct-2022	6.1	mxGraph v4.2.2 was discovered to contain a cross-site scripting (XSS) vulnerability via	N/A	A-JGR-MXGR-201022/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			the setTooltips() function. **CVE ID : CVE-2022-40440**		
Vendor: jiusi					
Product: jiusi_oa					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Oct-2022	9.8	A vulnerability classified as critical was found in Jiusi OA. Affected by this vulnerability is an unknown functionality of the file /jsoa/hntdCustomDesktopActionContent. The manipulation of the argument inforid leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-210709 was assigned to this vulnerability. **CVE ID : CVE-2022-3467**	N/A	A-JIU-JIUS-201022/430
Vendor: Johnsoncontrols					
Product: metasys_extended_application_and_data_server					
Affected Version(s): 12.0					
Improper Authentication	07-Oct-2022	6.5	On Metasys ADX Server version 12.0 running MVE, an Active Directory user could execute validated actions without providing a	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	A-JOH-META-201022/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			valid password when using MVE SMP UI. **CVE ID : CVE-2022-21936**		
Product: metasys_for_validated_environments					
Affected Version(s): -					
Improper Authentication	07-Oct-2022	6.5	On Metasys ADX Server version 12.0 running MVE, an Active Directory user could execute validated actions without providing a valid password when using MVE SMP UI. **CVE ID : CVE-2022-21936**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	A-JOH-META-201022/432
Vendor: js-beautify_project					
Product: js-beautify					
Affected Version(s): 1.13.7					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	11-Oct-2022	9.8	Prototype pollution vulnerability in beautify-web js-beautify 1.13.7 via the name variable in options.js. **CVE ID : CVE-2022-37609**	N/A	A-JS--JS-B-201022/433
Vendor: Libreoffice					
Product: libreoffice					
Affected Version(s): 7.4.0					
Improper Neutralization of Argument Delimiters in a	11-Oct-2022	6.3	LibreOffice supports Office URI Schemes to enable browser integration of LibreOffice with MS	https://www.libreoffice.org/about-us/security/advisories/CVE-2022-3140	A-LIB-LIBR-201022/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Argument Injection')			SharePoint server. An additional scheme 'vnd.libreoffice.command' specific to LibreOffice was added. In the affected versions of LibreOffice links using that scheme could be constructed to call internal macros with arbitrary arguments. Which when clicked on, or activated by document events, could result in arbitrary script execution without warning. This issue affects: The Document Foundation LibreOffice 7.4 versions prior to 7.4.1; 7.3 versions prior to 7.3.6. **CVE ID : CVE-2022-3140**		
Affected Version(s): From (including) 7.3.0 Up to (excluding) 7.3.6					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	11-Oct-2022	6.3	LibreOffice supports Office URI Schemes to enable browser integration of LibreOffice with MS SharePoint server. An additional scheme 'vnd.libreoffice.command' specific to	https://www.libreoffice.org/about-us/security/advisories/CVE-2022-3140	A-LIB-LIBR-201022/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LibreOffice was added. In the affected versions of LibreOffice links using that scheme could be constructed to call internal macros with arbitrary arguments. Which when clicked on, or activated by document events, could result in arbitrary script execution without warning. This issue affects: The Document Foundation LibreOffice 7.4 versions prior to 7.4.1; 7.3 versions prior to 7.3.6. **CVE ID : CVE-2022-3140**		
Vendor: lief-project					
Product: lief					
Affected Version(s): 0.12.1					
N/A	03-Oct-2022	6.5	A vulnerability in the LIEF::MachO::BinaryParser::init_and_parse function of LIEF v0.12.1 allows attackers to cause a denial of service (DOS) through a segmentation fault via a crafted MachO file.	N/A	A-LIE-LIEF-201022/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40922		
Vendor: Liferay					
Product: liferay_portal					
Affected Version(s): From (including) 7.0.0 Up to (including) 7.4.2					
Incorrect Default Permissions	07-Oct-2022	5.3	An insecure default in the component auth.login.prompt.enabled of Liferay Portal v7.0.0 through v7.4.2 allows attackers to enumerate usernames, site names, and pages. **CVE ID : CVE-2022-41414**	N/A	A-LIF-LIFE-201022/437
Vendor: Lighttpd					
Product: lighttpd					
Affected Version(s): From (including) 1.4.56 Up to (excluding) 1.4.67					
Missing Release of Memory after Effective Lifetime	06-Oct-2022	7.5	A resource leak in gw_backend.c in lighttpd 1.4.56 through 1.4.66 could lead to a denial of service (connection-slot exhaustion) after a large amount of anomalous TCP behavior by clients. It is related to RDHUP mishandling in certain HTTP/1.1 chunked situations. Use of mod_fastcgi is, for example, affected. This is fixed in 1.4.67.	https://git.lighttpd.net/lighttpd/lighttpd1.4/commit/b18de6f9264f914f7bf493abd3b6059343548e50	A-LIG-LIGH-201022/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41556		
Vendor: linaro					
Product: lava					
Affected Version(s): * Up to (excluding) 2022.10					
N/A	13-Oct-2022	8.8	In Linaro Automated Validation Architecture (LAVA) before 2022.10, there is dynamic code execution in lava_server/lavatable.py. Due to improper input sanitization, an anonymous user can force the lava-server-gunicorn service to execute user-provided code on the server. **CVE ID : CVE-2022-42902**	https://git.lavasoftware.org/lava/lava/-/commit/e66b74cd6c175ff8826b8f3431740963be228b52?merge_request_iid=1834, https://git.lavasoftware.org/lava/lava/-/merge_requests/1834	A-LIN-LAVA-201022/439
Vendor: Linuxfoundation					
Product: dapr_dashboard					
Affected Version(s): From (including) 0.1.0 Up to (including) 0.10.0					
N/A	03-Oct-2022	7.5	Dapr Dashboard v0.1.0 through v0.10.0 is vulnerable to Incorrect Access Control that allows attackers to obtain sensitive data. **CVE ID : CVE-2022-38817**	N/A	A-LIN-DAPR-201022/440
Product: dex					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.35.0					
Exposure of Sensitive Information to an Unauthorized Actor	06-Oct-2022	6.5	Dex is an identity service that uses OpenID Connect to drive authentication for other apps. Dex instances with public clients (and by extension, clients accepting tokens issued by those Dex instances) are affected by this vulnerability if they are running a version prior to 2.35.0. An attacker can exploit this vulnerability by making a victim navigate to a malicious website and guiding them through the OIDC flow, stealing the OAuth authorization code in the process. The authorization code then can be exchanged by the attacker for a token, gaining access to applications accepting that token. Version 2.35.0 has introduced a fix for this issue. Users are advised to upgrade. There are no	https://github.com/dexidp/dex/security/advisories/GHSA-vh7g-p26c-j2cw, https://github.com/dexidp/dex/commit/49471b14c8080ddb034d4855841123d378b7a634	A-LIN-DEX-201022/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2022-39222**		
Product: yocto					
Affected Version(s): 3.3					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	A-LIN-YOCT-201022/442
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425.	https://corp.mediatek.com/product-security-bulletin/October-2022	A-LIN-YOCT-201022/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32590		
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	A-LIN-YOCT-201022/444
Affected Version(s): 3.1					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	A-LIN-YOCT-201022/445
Improper Handling	07-Oct-2022	6.7	In wlan, there is a possible use after	https://corp.mediatek.com/pr	A-LIN-YOCT-201022/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Exceptional Conditions			free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	oduct-security-bulletin/October-2022	
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	A-LIN-YOCT-201022/447
Vendor: Linuxmint					
Product: warpinator					
Affected Version(s): * Up to (including) 1.2.14					
Improper Link Resolution Before File Access	10-Oct-2022	7.5	Warpinator through 1.2.14 allows access outside of an intended directory,	https://github.com/linuxmint/warpinator/commit/5244c33d4c109ede960	A-LIN-WARP-201022/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			as demonstrated by symbolic directory links. **CVE ID : CVE-2022-42725**	7b9d94461650410e2cddc, https://github.com/linuxmint/warpinator/commit/8bfd2f8b3f1b0c0f0a5a6d275702d107b9e08a94	
Vendor: melistechnology					
Product: melis-asset-manager					
Affected Version(s): * Up to (excluding) 5.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Oct-2022	7.5	MelisAssetManager provides deliveries of Melis Platform's assets located in every module's public folder. Attackers can read arbitrary files on affected versions of `melisplatform/melis-asset-manager`, leading to the disclosure of sensitive information. Conducting this attack does not require authentication. Users should immediately upgrade to `melisplatform/melis-asset-manager` >= 5.0.1. This issue was addressed by restricting access to files to intended directories only.	https://github.com/melisplatform/melis-asset-manager/security/advisories/GHSA-7fj2-rrq6-rphq, https://github.com/melisplatform/melis-asset-manager/commit/a0f75918c049aff78953a0bc91c585153595d1bd	A-MEL-MELI-201022/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39296		
Product: meliscms					
Affected Version(s): * Up to (excluding) 5.0.1					
Deserialization of Untrusted Data	12-Oct-2022	9.8	MelisCms provides a full CMS for Melis Platform, including templating system, drag'n'drop of plugins, SEO and many administration tools. Attackers can deserialize arbitrary data on affected versions of `melisplatform/melis-cms`, and ultimately leads to the execution of arbitrary PHP code on the system. Conducting this attack does not require authentication. Users should immediately upgrade to `melisplatform/melis-cms` >= 5.0.1. This issue was addressed by restricting allowed classes when deserializing user-controlled data. **CVE ID : CVE-2022-39297**	https://github.com/melisplatform/melis-cms/commit/d124b2474699a679a24ec52620cadceb3d4cec11, https://github.com/melisplatform/melis-cms/security/advisories/GHSA-m3m3-6gww-7gj9	A-MEL-MELI-201022/450
Deserialization of	12-Oct-2022	9.8	MelisFront is the engine that displays website hosted on	https://github.com/melisplatform/melis-	A-MEL-MELI-201022/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			Melis Platform. It deals with showing pages, plugins, URL rewritting, search optimization and SEO, etc. Attackers can deserialize arbitrary data on affected versions of `melisplatform/melis-front`, and ultimately leads to the execution of arbitrary PHP code on the system. Conducting this attack does not require authentication. Users should immediately upgrade to `melisplatform/melis-front` >= 5.0.1. This issue was addressed by restricting allowed classes when deserializing user-controlled data. **CVE ID : CVE-2022-39298**	front/commit/89ae612d5f1f7aa2fb621ee8de27dffe1feb851e, https://github.com/melisplatform/melis-front/security/advisories/GHSA-h479-2mv4-5c26	
Vendor: merchandise_online_store_project					
Product: merchandise_online_store					
Affected Version(s): 1.0					
Improper Privilege Management	11-Oct-2022	8.8	A Vertical Privilege Escalation issue in Merchandise Online Store v.1.0 allows an attacker to get access to the admin dashboard.	N/A	A-MER-MERC-201022/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42238		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A Stored XSS issue in Merchandise Online Store v.1.0 allows to injection of Arbitrary JavaScript in edit account form. **CVE ID : CVE-2022-42236**	N/A	A-MER-MERC-201022/453
Vendor: metaslider					
Product: slider\,_gallery\,_and_carousel					
Affected Version(s): * Up to (excluding) 3.27.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2022	4.8	The Slider, Gallery, and Carousel by MetaSlider WordPress plugin before 3.27.9 does not sanitise and escape some of its Gallery Image parameters, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2823**	N/A	A-MET-SLID-201022/454
Vendor: metroui					
Product: metro_ui					
Affected Version(s): From (including) 4.4.0 Up to (including) 4.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	Metro UI v4.4.0 to v4.5.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Javascript function. **CVE ID : CVE-2022-41376**	N/A	A-MET-METR-201022/455
Vendor: Microsoft					
Product: .net					
Affected Version(s): 6.0.0					
N/A	11-Oct-2022	7.8	NuGet Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41032	A-MIC-.NET-201022/456
Product: .net_core					
Affected Version(s): 3.1					
N/A	11-Oct-2022	7.8	NuGet Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41032	A-MIC-.NET-201022/457
Product: 365_apps					
Affected Version(s): -					
N/A	11-Oct-2022	7.8	Microsoft Office Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38048	A-MIC-365_-201022/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38049	A-MIC-365_-201022/459
N/A	11-Oct-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41031	A-MIC-365_-201022/460
N/A	11-Oct-2022	6.5	Microsoft Office Spoofing Vulnerability. **CVE ID : CVE-2022-38001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38001	A-MIC-365_-201022/461
Product: azure_arc-enabled_kubernetes					
Affected Version(s): 1.5.8					
Improper Privilege Management	11-Oct-2022	10	Azure Arc-enabled Kubernetes cluster Connect Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37968	A-MIC-AZUR-201022/462
Affected Version(s): 1.6.19					
Improper Privilege Management	11-Oct-2022	10	Azure Arc-enabled Kubernetes cluster Connect Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37968	A-MIC-AZUR-201022/463
Affected Version(s): 1.7.18					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-Oct-2022	10	Azure Arc-enabled Kubernetes cluster Connect Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37968	A-MIC-AZUR-201022/464
Affected Version(s): 1.8.11					
Improper Privilege Management	11-Oct-2022	10	Azure Arc-enabled Kubernetes cluster Connect Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37968	A-MIC-AZUR-201022/465
Product: azure_service_fabric					
Affected Version(s): -					
N/A	11-Oct-2022	4.8	Service Fabric Explorer Spoofing Vulnerability. **CVE ID : CVE-2022-35829**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35829	A-MIC-AZUR-201022/466
Product: azure_stack_edge					
Affected Version(s): -					
Improper Privilege Management	11-Oct-2022	10	Azure Arc-enabled Kubernetes cluster Connect Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37968**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37968	A-MIC-AZUR-201022/467
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 106.0.1370.34					
Concurrent Execution using Shared	11-Oct-2022	5.3	Microsoft Edge (Chromium-based) Spoofing Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-EDGE-201022/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			**CVE ID : CVE-2022-41035**	guidance/advisory/CVE-2022-41035	
Product: exchange_server					
Affected Version(s): 2019					
Improper Privilege Management	03-Oct-2022	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040	A-MIC-EXCH-201022/469
N/A	03-Oct-2022	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41082**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082	A-MIC-EXCH-201022/470
Affected Version(s): 2013					
Improper Privilege Management	03-Oct-2022	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040	A-MIC-EXCH-201022/471
N/A	03-Oct-2022	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41082**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082	A-MIC-EXCH-201022/472
Affected Version(s): 2016					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	03-Oct-2022	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040	A-MIC-EXCH-201022/473
N/A	03-Oct-2022	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41082**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082	A-MIC-EXCH-201022/474
Product: jupyter					
Affected Version(s): * Up to (excluding) 2022.9.110					
N/A	11-Oct-2022	7.8	Visual Studio Code Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41083**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41083	A-MIC-JUPY-201022/475
Product: malware_protection_engine					
Affected Version(s): * Up to (excluding) 1.1.19700.2					
Improper Privilege Management	11-Oct-2022	7.1	Microsoft Windows Defender Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37971**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37971	A-MIC-MALW-201022/476
Product: office					
Affected Version(s): 2019					
N/A	11-Oct-2022	7.8	Microsoft Office Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-OFFI-201022/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-38048	
N/A	11-Oct-2022	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38049	A-MIC-OFFI-201022/478
N/A	11-Oct-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41031	A-MIC-OFFI-201022/479
N/A	11-Oct-2022	6.5	Microsoft Office Spoofing Vulnerability. **CVE ID : CVE-2022-38001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38001	A-MIC-OFFI-201022/480
N/A	11-Oct-2022	5.3	Microsoft Office Information Disclosure Vulnerability. **CVE ID : CVE-2022-41043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41043	A-MIC-OFFI-201022/481
Affected Version(s): 2013					
N/A	11-Oct-2022	7.8	Microsoft Office Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38048	A-MIC-OFFI-201022/482
Affected Version(s): 2016					
N/A	11-Oct-2022	7.8	Microsoft Office Remote Code	https://portal.msrc.microsoft.	A-MIC-OFFI-201022/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability. **CVE ID : CVE-2022-38048**	com/en-US/security-guidance/advisory/CVE-2022-38048	
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	11-Oct-2022	7.8	Microsoft Office Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38048	A-MIC-OFFI-201022/484
N/A	11-Oct-2022	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38049	A-MIC-OFFI-201022/485
N/A	11-Oct-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41031	A-MIC-OFFI-201022/486
N/A	11-Oct-2022	6.5	Microsoft Office Spoofing Vulnerability. **CVE ID : CVE-2022-38001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38001	A-MIC-OFFI-201022/487
N/A	11-Oct-2022	5.3	Microsoft Office Information Disclosure Vulnerability. **CVE ID : CVE-2022-41043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-OFFI-201022/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-41043	
Product: sharepoint_enterprise_server					
Affected Version(s): 2013					
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41036, CVE-2022-41037, CVE-2022-41038. **CVE ID : CVE-2022-38053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38053	A-MIC-SHAR-201022/489
Affected Version(s): 2016					
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41036, CVE-2022-41037, CVE-2022-41038. **CVE ID : CVE-2022-38053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38053	A-MIC-SHAR-201022/490
Product: sharepoint_foundation					
Affected Version(s): 2013					
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41036, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38053	A-MIC-SHAR-201022/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			41037, CVE-2022-41038. **CVE ID : CVE-2022-38053**		
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41037, CVE-2022-41038. **CVE ID : CVE-2022-41036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41036	A-MIC-SHAR-201022/492
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41036, CVE-2022-41038. **CVE ID : CVE-2022-41037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41037	A-MIC-SHAR-201022/493
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41036, CVE-2022-41037. **CVE ID : CVE-2022-41038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41038	A-MIC-SHAR-201022/494
Product: sharepoint_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2019					
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41036, CVE-2022-41037, CVE-2022-41038. **CVE ID : CVE-2022-38053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38053	A-MIC-SHAR-201022/495
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41037, CVE-2022-41038. **CVE ID : CVE-2022-41036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41036	A-MIC-SHAR-201022/496
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41036, CVE-2022-41038. **CVE ID : CVE-2022-41037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41037	A-MIC-SHAR-201022/497
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-SHAR-201022/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-38053, CVE-2022-41036, CVE-2022-41037. **CVE ID : CVE-2022-41038**	ory/CVE-2022-41038	
Affected Version(s): -					
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41036, CVE-2022-41037, CVE-2022-41038. **CVE ID : CVE-2022-38053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38053	A-MIC-SHAR-201022/499
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41037, CVE-2022-41038. **CVE ID : CVE-2022-41036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41036	A-MIC-SHAR-201022/500
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41037	A-MIC-SHAR-201022/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			41036, CVE-2022-41038. **CVE ID : CVE-2022-41037**		
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41036, CVE-2022-41037. **CVE ID : CVE-2022-41038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41038	A-MIC-SHAR-201022/502
Affected Version(s): 2013					
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41037, CVE-2022-41038. **CVE ID : CVE-2022-41036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41036	A-MIC-SHAR-201022/503
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41036, CVE-2022-41038. **CVE ID : CVE-2022-41037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41037	A-MIC-SHAR-201022/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41036, CVE-2022-41037. **CVE ID : CVE-2022-41038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41038	A-MIC-SHAR-201022/505
Affected Version(s): 2016					
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41037, CVE-2022-41038. **CVE ID : CVE-2022-41036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41036	A-MIC-SHAR-201022/506
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38053, CVE-2022-41036, CVE-2022-41038. **CVE ID : CVE-2022-41037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41037	A-MIC-SHAR-201022/507
N/A	11-Oct-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-SHAR-201022/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-38053, CVE-2022-41036, CVE-2022-41037. **CVE ID : CVE-2022-41038**	ory/CVE-2022-41038	
Product: visual_studio_2019					
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.9.26					
N/A	11-Oct-2022	7.8	NuGet Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41032	A-MIC-VISU-201022/509
Affected Version(s): From (including) 16.10.0 Up to (excluding) 16.11.20					
N/A	11-Oct-2022	7.8	NuGet Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41032	A-MIC-VISU-201022/510
Product: visual_studio_2022					
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.15					
N/A	11-Oct-2022	7.8	NuGet Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41032	A-MIC-VISU-201022/511
Affected Version(s): From (including) 17.2.0 Up to (excluding) 17.2.9					
N/A	11-Oct-2022	7.8	NuGet Client Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-VISU-201022/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41032	ory/CVE-2022-41032	
Affected Version(s): From (including) 17.3 Up to (excluding) 17.3.6					
N/A	11-Oct-2022	7.8	NuGet Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41032	A-MIC-VISU-201022/513
Affected Version(s): From (including) 17.3 Up to (excluding) 17.3.7					
N/A	11-Oct-2022	7.8	NuGet Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41032	A-MIC-VISU-201022/514
Product: visual_studio_code					
Affected Version(s): -					
N/A	11-Oct-2022	7.4	Visual Studio Code Information Disclosure Vulnerability. **CVE ID : CVE-2022-41042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41042	A-MIC-VISU-201022/515
Affected Version(s): * Up to (excluding) 1.72.1					
N/A	11-Oct-2022	7.8	Visual Studio Code Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41034	A-MIC-VISU-201022/516
Vendor: Misp-project					
Product: malware_information_sharing_platform					
Affected Version(s): * Up to (excluding) 2.4.164					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	10-Oct-2022	4.3	app/Controller/UsersController.php in MISP before 2.4.164 allows attackers to discover role names (this is information that only the site admin should have). **CVE ID : CVE-2022-42724**	https://github.com/MISP/MISP/commit/934b9cd4fc6d6378ad349ea630ad9f1319ac82f5	A-MIS-MALW-201022/517
Vendor: mockery_project					
Product: mockery					
Affected Version(s): 2.1.0					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	12-Oct-2022	9.8	Prototype pollution vulnerability in function enable in mockery.js in mfncooper mockery commit 822f0566fd6d72af8c943ae5ca2aa92e516aa2cf via the key variable in mockery.js. **CVE ID : CVE-2022-37614**	N/A	A-MOC-MOCK-201022/518
Vendor: mojoportal					
Product: mojoportal					
Affected Version(s): 2.7.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Oct-2022	6.5	mojoPortal v2.7 was discovered to contain a path traversal vulnerability via the "f" parameter at /DesignTools/CssEditor.aspx. This vulnerability allows authenticated	N/A	A-MOJ-MOJO-201022/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to read arbitrary files in the system. **CVE ID : CVE-2022-40123**		
Vendor: Moodle					
Product: moodle					
Affected Version(s): From (including) 3.11.0 Up to (excluding) 3.11.9					
Cross-Site Request Forgery (CSRF)	06-Oct-2022	8.8	Enabling and disabling installed H5P libraries did not include the necessary token to prevent a CSRF risk. **CVE ID : CVE-2022-2986**	https://bugzilla.redhat.com/show_bug.cgi?id=2121360, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-75326	A-MOO-MOOD-201022/520
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.3					
Cross-Site Request Forgery (CSRF)	06-Oct-2022	8.8	Enabling and disabling installed H5P libraries did not include the necessary token to prevent a CSRF risk. **CVE ID : CVE-2022-2986**	https://bugzilla.redhat.com/show_bug.cgi?id=2121360, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-75326	A-MOO-MOOD-201022/521
Vendor: Mybb					
Product: mybb					
Affected Version(s): * Up to (excluding) 1.8.31					
Improper Neutralization of Special Elements in Output Used by a Downstrea	06-Oct-2022	7.2	MyBB is a free and open source forum software. The _Mail Settings_ ? Additional Parameters for PHP's mail() function	https://mybb.com/versions/1.8.31/, https://github.com/mybb/mybb/security/advisories/GHSA-hxhm-rq9f-	A-MYB-MYBB-201022/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			mail_parameters setting value, in connection with the configured mail program's options and behavior, may allow access to sensitive information and Remote Code Execution (RCE). The vulnerable module requires Admin CP access with the `_Can manage settings?_` permission and may depend on configured file permissions. MyBB 1.8.31 resolves this issue with the commit `0cd318136a`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-39265**	7xj7, https://github.com/mybb/mybb/commit/0cd318136a10b029bb5c8a8f6dddf39d87519797	
Vendor: Najeebmedia					
Product: frontend_file_manager					
Affected Version(s): * Up to (excluding) 21.3					
Unrestricted Upload of File with Dangerous Type	03-Oct-2022	8.8	The Frontend File Manager Plugin WordPress plugin before 21.3 allows any authenticated users, such as subscriber, to rename a file to an	N/A	A-NAJ-FRON-201022/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary extension, like PHP, which could allow them to basically be able to upload arbitrary files on the server and achieve RCE **CVE ID : CVE-2022-3125**		
Missing Authorization	03-Oct-2022	5.3	The Frontend File Manager Plugin WordPress plugin before 21.3 allows any unauthenticated user to rename uploaded files from users. Furthermore, due to the lack of validation in the destination filename, this could allow allow them to change the content of arbitrary files on the web server **CVE ID : CVE-2022-3124**	N/A	A-NAJ-FRON-201022/524
Vendor: Nasm					
Product: netwide_assembler					
Affected Version(s): 2.16					
Out-of-bounds Write	03-Oct-2022	5.5	nasm v2.16 was discovered to contain a stack overflow in the Ndisasm component **CVE ID : CVE-2022-41420**	https://bugzilla.nasm.us/show_bug.cgi?id=3392810	A-NAS-NETW-201022/525
Vendor: nedi					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nedi					
Affected Version(s): * Up to (including) 1.0.7					
Observable Discrepancy	06-Oct-2022	9.1	In certain Nedi products, a vulnerability in the web UI of NeDi login & Community login could allow an unauthenticated, remote attacker to affect the integrity of a device via a User Enumeration vulnerability. The vulnerability is due to insecure design, where a difference in forgot password utility could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users. This affects NeDi 1.0.7 for OS X 1.0.7 <= and NeDi for Suse 1.0.7 <= and NeDi for FreeBSD 1.0.7 <=. **CVE ID : CVE-2022-40895**	http://forum.nedi.ch/index.php, https://www.nedi.ch/	A-NED-NEDI-201022/526
Affected Version(s): 1.0.7					
Observable Discrepancy	06-Oct-2022	9.1	In certain Nedi products, a vulnerability in the web UI of NeDi login & Community login could allow an unauthenticated, remote attacker to	http://forum.nedi.ch/index.php, https://www.nedi.ch/	A-NED-NEDI-201022/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect the integrity of a device via a User Enumeration vulnerability. The vulnerability is due to insecure design, where a difference in forgot password utility could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users. This affects NeDi 1.0.7 for OS X 1.0.7 <= and NeDi for Suse 1.0.7 <= and NeDi for FreeBSD 1.0.7 <=. **CVE ID : CVE-2022-40895**		
Vendor: newsletter_subscribe_\(popup_\+_regular_module\)_project					
Product: newsletter_subscribe_\(popup_\+_regular_module\)					
Affected Version(s): 4.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Oct-2022	9.8	OpenCart 3.x Newsletter Custom Popup was discovered to contain a SQL injection vulnerability via the email parameter at index.php?route=extension/module/so_newletter_custom_popup/newsletter. **CVE ID : CVE-2022-41403**	N/A	A-NEW-NEWS-201022/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: node_saml_project					
Product: node_saml					
Affected Version(s): * Up to (excluding) 4.0.0					
Improper Verification of Cryptographic Signature	13-Oct-2022	8.1	node SAML is a SAML 2.0 library based on the SAML implementation of passport-saml. A remote attacker may be able to bypass SAML authentication on a website using passport-saml. A successful attack requires that the attacker is in possession of an arbitrary IDP signed XML element. Depending on the IDP used, fully unauthenticated attacks (e.g without access to a valid user) might also be feasible if generation of a signed message can be triggered. Users should upgrade to node-saml version 4.0.0-beta5 or newer. Disabling SAML authentication may be done as a workaround. **CVE ID : CVE-2022-39300**	https://github.com/node-saml/node-saml/commit/c1f275c289c01921e58f5c70ce0fdbc5287e5fbe, https://github.com/node-saml/node-saml/security/advisories/GHSA-5p8w-2mvw-38pv	A-NOD-NODE-201022/529
Affected Version(s): 4.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	13-Oct-2022	8.1	node SAML is a SAML 2.0 library based on the SAML implementation of passport-saml. A remote attacker may be able to bypass SAML authentication on a website using passport-saml. A successful attack requires that the attacker is in possession of an arbitrary IDP signed XML element. Depending on the IDP used, fully unauthenticated attacks (e.g without access to a valid user) might also be feasible if generation of a signed message can be triggered. Users should upgrade to node-saml version 4.0.0-beta5 or newer. Disabling SAML authentication may be done as a workaround. **CVE ID : CVE-2022-39300**	https://github.com/node-saml/node-saml/commit/c1f275c289c01921e58f5c70ce0fdbc5287e5fbe, https://github.com/node-saml/node-saml/security/advisories/GHSA-5p8w-2mvw-38pv	A-NOD-NODE-201022/530
Vendor: nps_project					
Product: nps					
Affected Version(s): From (including) 0.19.0 Up to (including) 0.26.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	06-Oct-2022	9.8	NPS before v0.26.10 was discovered to contain an authentication bypass vulnerability via constantly generating and sending the Auth key and Timestamp parameters. **CVE ID : CVE-2022-40494**	N/A	A-NPS-NPS-201022/531
Vendor: ocomon_project					
Product: ocomon					
Affected Version(s): 4.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Oct-2022	9.8	OcoMon v4.0 was discovered to contain a SQL injection vulnerability via the cod parameter at download.php. **CVE ID : CVE-2022-41390**	N/A	A-OCO-OCOM-201022/532
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Oct-2022	9.8	OcoMon v4.0 was discovered to contain a SQL injection vulnerability via the cod parameter at showImg.php. **CVE ID : CVE-2022-41391**	N/A	A-OCO-OCOM-201022/533
Vendor: octopus					
Product: octopus_server					
Affected Version(s): From (including) 2022.1.2121 Up to (including) 2022.1.3135					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	13-Oct-2022	6.5	In affected versions of Octopus Server it is possible to reveal information about teams via the API due to an Insecure Direct Object Reference (IDOR) vulnerability **CVE ID : CVE-2022-2828**	https://advisories.octopus.com/post/2022/sa2022-19/	A-OCT-OCTO-201022/534
Affected Version(s): From (including) 2022.2.0 Up to (including) 2022.2.7897					
Authorization Bypass Through User-Controlled Key	13-Oct-2022	6.5	In affected versions of Octopus Server it is possible to reveal information about teams via the API due to an Insecure Direct Object Reference (IDOR) vulnerability **CVE ID : CVE-2022-2828**	https://advisories.octopus.com/post/2022/sa2022-19/	A-OCT-OCTO-201022/535
Affected Version(s): From (including) 2022.2.6729 Up to (excluding) 2022.2.7897					
Inadequate Encryption Strength	06-Oct-2022	5.3	In affected versions of Octopus Server it was identified that the same encryption process was used for both encrypting session cookies and variables. **CVE ID : CVE-2022-2781**	https://advisories.octopus.com/post/2022/sa2022-16/	A-OCT-OCTO-201022/536
Insufficient Session Expiration	06-Oct-2022	5.3	In affected versions of Octopus Server it was identified that a session cookie could be used as the CSRF token	https://advisories.octopus.com/post/2022/sa2022-17/	A-OCT-OCTO-201022/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2783		
Affected Version(s): From (including) 2022.2.6729 Up to (excluding) 2022.2.7934					
N/A	12-Oct-2022	5.3	In affected versions of Octopus Server it was identified that when a sensitive value is a substring of another value, sensitive value masking will only partially work. **CVE ID : CVE-2022-2720**	https://advisories.octopus.com/post/2022/sa2022-18/	A-OCT-OCTO-201022/538
Affected Version(s): From (including) 2022.3.0 Up to (including) 2022.3.10586					
Authorization Bypass Through User-Controlled Key	13-Oct-2022	6.5	In affected versions of Octopus Server it is possible to reveal information about teams via the API due to an Insecure Direct Object Reference (IDOR) vulnerability **CVE ID : CVE-2022-2828**	https://advisories.octopus.com/post/2022/sa2022-19/	A-OCT-OCTO-201022/539
Affected Version(s): From (including) 2022.3.348 Up to (excluding) 2022.3.10586					
N/A	12-Oct-2022	5.3	In affected versions of Octopus Server it was identified that when a sensitive value is a substring of another value, sensitive value masking will only partially work. **CVE ID : CVE-2022-2720**	https://advisories.octopus.com/post/2022/sa2022-18/	A-OCT-OCTO-201022/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	06-Oct-2022	5.3	In affected versions of Octopus Server it was identified that the same encryption process was used for both encrypting session cookies and variables. **CVE ID : CVE-2022-2781**	https://advisories.octopus.com/post/2022/sa2022-16/	A-OCT-OCTO-201022/541
Insufficient Session Expiration	06-Oct-2022	5.3	In affected versions of Octopus Server it was identified that a session cookie could be used as the CSRF token **CVE ID : CVE-2022-2783**	https://advisories.octopus.com/post/2022/sa2022-17/	A-OCT-OCTO-201022/542
Affected Version(s): From (including) 3.12.0 Up to (excluding) 2022.1.3154					
Insufficient Session Expiration	06-Oct-2022	5.3	In affected versions of Octopus Server it was identified that a session cookie could be used as the CSRF token **CVE ID : CVE-2022-2783**	https://advisories.octopus.com/post/2022/sa2022-17/	A-OCT-OCTO-201022/543
Affected Version(s): From (including) 3.16.4 Up to (excluding) 2022.1.3154					
N/A	12-Oct-2022	5.3	In affected versions of Octopus Server it was identified that when a sensitive value is a substring of another value, sensitive value masking will only partially work. **CVE ID : CVE-2022-2720**	https://advisories.octopus.com/post/2022/sa2022-18/	A-OCT-OCTO-201022/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 3.2.10 Up to (excluding) 2022.1.3154					
Inadequate Encryption Strength	06-Oct-2022	5.3	In affected versions of Octopus Server it was identified that the same encryption process was used for both encrypting session cookies and variables. **CVE ID : CVE-2022-2781**	https://advisories.octopus.com/post/2022/sa2022-16/	A-OCT-OCTO-201022/545
Vendor: Omron					
Product: cx-programmer					
Affected Version(s): * Up to (including) 9.78					
Out-of-bounds Write	06-Oct-2022	9.8	OMRON CX-Programmer 9.78 and prior is vulnerable to an Out-of-Bounds Write, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3396**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-277-04	A-OMR-CX-P-201022/546
Out-of-bounds Write	06-Oct-2022	9.8	OMRON CX-Programmer 9.78 and prior is vulnerable to an Out-of-Bounds Write, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3397**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-277-04	A-OMR-CX-P-201022/547
Out-of-bounds Write	06-Oct-2022	9.8	OMRON CX-Programmer 9.78 and prior is vulnerable to an	https://www.cisa.gov/uscert/i	A-OMR-CX-P-201022/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out-of-Bounds Write, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3398**	cs/advisories/icsa-22-277-04	
Vendor: online_birth_certificate_management_system_project					
Product: online_birth_certificate_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Oct-2022	5.4	Online Birth Certificate Management System version 1.0 suffers from a persistent Cross Site Scripting (XSS) vulnerability. **CVE ID : CVE-2022-42069**	N/A	A-ONL-ONLI-201022/549
Vendor: online_diagnostic_lab_management_system_project					
Product: online_diagnostic_lab_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Oct-2022	9.8	Online Diagnostic Lab Management System version 1.0 remote exploit that bypasses login with SQL injection and then uploads a shell. **CVE ID : CVE-2022-42064**	N/A	A-ONL-ONLI-201022/550
Unrestricted Upload of File with Dangerous Type	07-Oct-2022	7.2	An arbitrary file upload vulnerability in the component /php_action/editFile.php of Online Diagnostic Lab	N/A	A-ONL-ONLI-201022/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-41512**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /diagnostic/edittest.php. **CVE ID : CVE-2022-41513**	N/A	A-ONL-ONLI-201022/552
Unrestricted Upload of File with Dangerous Type	13-Oct-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via the component /php_action/editProductImage.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-41533**	N/A	A-ONL-ONLI-201022/553
Unrestricted Upload of File with Dangerous Type	13-Oct-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain an	N/A	A-ONL-ONLI-201022/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary file upload vulnerability via the component /php_action/createOrder.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-41534**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	7.2	Online Diagnostic Lab Management System v1.0 is vulnerable to SQL Injection via /diagnostic/editclient.php?id=. **CVE ID : CVE-2022-42073**	N/A	A-ONL-ONLI-201022/555
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	7.2	Online Diagnostic Lab Management System v1.0 is vulnerable to SQL Injection via /diagnostic/editcategory.php?id=. **CVE ID : CVE-2022-42074**	N/A	A-ONL-ONLI-201022/556
Vendor: online_leave_management_system_project					
Product: online_leave_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL	06-Oct-2022	7.2	Online Leave Management System v1.0 was discovered to contain a SQL injection vulnerability via	N/A	A-ONL-ONLI-201022/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			the id parameter at /leave_system/classes/Master.php?f=delete_department. **CVE ID : CVE-2022-41355**		
Unrestricted Upload of File with Dangerous Type	07-Oct-2022	7.2	An arbitrary file upload vulnerability in the component /leave_system/classes/Users.php?f=save of Online Leave Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-41379**	N/A	A-ONL-ONLI-201022/558
Vendor: online_pet_shop_we_app_project					
Product: online_pet_shop_we_app					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Oct-2022	9.8	Online Pet Shop We App v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=orders/view_order. **CVE ID : CVE-2022-41408**	N/A	A-ONL-ONLI-201022/559
Improper Neutralization of Special Elements used in an SQL	07-Oct-2022	7.2	Online Pet Shop We App v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at	N/A	A-ONL-ONLI-201022/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			/pet_shop/admin/?page=maintenance/manage_category. **CVE ID : CVE-2022-41377**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	7.2	Online Pet Shop We App v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /pet_shop/admin/?page=inventory/manage_inventory. **CVE ID : CVE-2022-41378**	N/A	A-ONL-ONLI-201022/561
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Oct-2022	7.2	Online Pet Shop We App v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=orders/view_order. **CVE ID : CVE-2022-41407**	N/A	A-ONL-ONLI-201022/562
Vendor: Openssl					
Product: openssl					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.6					
NULL Pointer Dereference	11-Oct-2022	7.5	OpenSSL supports creating a custom cipher via the legacy EVP_CIPHER_meth_new() function and associated function calls. This function was deprecated in OpenSSL 3.0 and	https://www.openssl.org/news/secadv/20221011.txt, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=5485c56679d7c49b96e8fc8c	A-OPE-OPEN-201022/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application authors are instead encouraged to use the new provider mechanism in order to implement custom ciphers. OpenSSL versions 3.0.0 to 3.0.5 incorrectly handle legacy custom ciphers passed to the EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() and EVP_CipherInit_ex2() functions (as well as other similarly named encryption and decryption initialisation functions). Instead of using the custom cipher directly it incorrectly tries to fetch an equivalent cipher from the available providers. An equivalent cipher is found based on the NID passed to EVP_CIPHER_meth_new(). This NID is supposed to represent the unique NID for a given cipher. However it is possible for an application to incorrectly pass	a708b0b7e7c03c4b	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NID_undef as this value in the call to EVP_CIPHER_meth_new(). When NID_undef is used in this way the OpenSSL encryption/decryption initialisation function will match the NULL cipher as being equivalent and will fetch this from the available providers. This will succeed if the default provider has been loaded (or if a third party provider has been loaded that offers this cipher). Using the NULL cipher means that the plaintext is emitted as the ciphertext. Applications are only affected by this issue if they call EVP_CIPHER_meth_new() using NID_undef and subsequently use it in a call to an encryption/decryption initialisation function. Applications that only use SSL/TLS are not impacted by this issue. Fixed in OpenSSL 3.0.6		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Affected 3.0.0-3.0.5). **CVE ID : CVE-2022-3358**		
Vendor: open_source_sacco_management_system_project					
Product: open_source_sacco_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	7.2	Open Source SACCO Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /sacco_shield/ajax.php?action=delete_loan. **CVE ID : CVE-2022-41514**	N/A	A-OPE-OPEN-201022/564
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	7.2	Open Source SACCO Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /sacco_shield/ajax.php?action=delete_payment. **CVE ID : CVE-2022-41515**	N/A	A-OPE-OPEN-201022/565
Improper Neutralization of Special Elements used in an SQL Command	12-Oct-2022	7.2	Open Source SACCO Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at	N/A	A-OPE-OPEN-201022/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			/sacco_shield/ajax.php?action=delete_borrower. **CVE ID : CVE-2022-41530**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Oct-2022	7.2	Open Source SACCO Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /sacco_shield/ajax.php?action=delete_plan. **CVE ID : CVE-2022-41532**	N/A	A-OPE-OPEN-201022/567
Vendor: orchardcore					
Product: orchardcore					
Affected Version(s): From (including) 0.0.1 Up to (excluding) 1.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2022	5.4	In OrchardCore rc1-11259 to v1.2.2 vulnerable to HTML injection, allow an authenticated user with an editor security role to inject a persistent HTML modal dialog component into the dashboard that will affect admin users. **CVE ID : CVE-2022-32173**	https://github.com/OrchardCMS/OrchardCore/commit/0163c88ddeaca39815d7e6e5ea1c8391085cc136	A-ORC-ORCH-201022/568
Vendor: otfcc_project					
Product: otfcc					
Affected Version(s): * Up to (including) 0.10.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b5567. **CVE ID : CVE-2022-35040**	N/A	A-OTF-OTFC-201022/569
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b558f. **CVE ID : CVE-2022-35041**	N/A	A-OTF-OTFC-201022/570
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x4adb11. **CVE ID : CVE-2022-35042**	N/A	A-OTF-OTFC-201022/571
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6c08a6. **CVE ID : CVE-2022-35043**	N/A	A-OTF-OTFC-201022/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x617087. **CVE ID : CVE-2022-35044**	N/A	A-OTF-OTFC-201022/573
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b0d63. **CVE ID : CVE-2022-35045**	N/A	A-OTF-OTFC-201022/574
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b0466. **CVE ID : CVE-2022-35046**	N/A	A-OTF-OTFC-201022/575
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b05aa. **CVE ID : CVE-2022-35047**	N/A	A-OTF-OTFC-201022/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b0b2c. **CVE ID : CVE-2022-35048**	N/A	A-OTF-OTFC-201022/577
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b03b5. **CVE ID : CVE-2022-35049**	N/A	A-OTF-OTFC-201022/578
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b04de. **CVE ID : CVE-2022-35050**	N/A	A-OTF-OTFC-201022/579
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b55af. **CVE ID : CVE-2022-35051**	N/A	A-OTF-OTFC-201022/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b84b1. **CVE ID : CVE-2022-35052**	N/A	A-OTF-OTFC-201022/581
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x61731f. **CVE ID : CVE-2022-35053**	N/A	A-OTF-OTFC-201022/582
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6171b2. **CVE ID : CVE-2022-35054**	N/A	A-OTF-OTFC-201022/583
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6c0473. **CVE ID : CVE-2022-35055**	N/A	A-OTF-OTFC-201022/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b0478. **CVE ID : CVE-2022-35056**	N/A	A-OTF-OTFC-201022/585
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b05ce. **CVE ID : CVE-2022-35058**	N/A	A-OTF-OTFC-201022/586
Out-of-bounds Write	14-Oct-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6c0414. **CVE ID : CVE-2022-35059**	N/A	A-OTF-OTFC-201022/587
Vendor: panini					
Product: everest_engine					
Affected Version(s): 2.0.4					
Unquoted Search Path or Element	07-Oct-2022	7.8	Panini Everest Engine 2.0.4 allows unprivileged users to create a file named Everest.exe in the %PROGRAMDATA%\Panini folder.	https://www.panini.com/en/news-events/panini-patents-revolutionary-new-%E2%80%9Ce	A-PAN-EVER-201022/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This leads to privilege escalation because a service, running as SYSTEM, uses the unquoted path of %PROGRAMDATA%\Panini\Everest Engine\EverestEngine.exe and therefore a Trojan horse %PROGRAMDATA%\Panini\Everest.exe may be executed instead of the intended vendor-supplied EverestEngine.exe file. **CVE ID : CVE-2022-39959**	verest%E2%80%9D-architecture	
Vendor: passport-saml_project					
Product: passport-saml					
Affected Version(s): 4.0.0					
Improper Verification of Cryptographic Signature	12-Oct-2022	8.1	Passport-SAML is a SAML 2.0 authentication provider for Passport, the Node.js authentication library. A remote attacker may be able to bypass SAML authentication on a website using passport-saml. A successful attack requires that the attacker is in	https://github.com/node-saml/passport-saml/security/advisories/GHSA-m974-647v-whv7, https://github.com/node-saml/passport-saml/commit/8b7e3f5a91c8e5ac7e890a0c90bc7491ce33155e	A-PAS-PASS-201022/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possession of an arbitrary IDP signed XML element. Depending on the IDP used, fully unauthenticated attacks (e.g without access to a valid user) might also be feasible if generation of a signed message can be triggered. Users should upgrade to passport-saml version 3.2.2 or newer. The issue was also present in the beta releases of `node-saml` before version 4.0.0-beta.5. If you cannot upgrade, disabling SAML authentication may be done as a workaround. **CVE ID : CVE-2022-39299**		
Affected Version(s): * Up to (excluding) 3.2.2					
Improper Verification of Cryptographic Signature	12-Oct-2022	8.1	Passport-SAML is a SAML 2.0 authentication provider for Passport, the Node.js authentication library. A remote attacker may be able to bypass SAML authentication on a	https://github.com/node-saml/passport-saml/security/advisories/GHSA-m974-647v-whv7, https://github.com/node-saml/passport-saml/commit/8b7e3f5a91c8e5	A-PAS-PASS-201022/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			website using passport-saml. A successful attack requires that the attacker is in possession of an arbitrary IDP signed XML element. Depending on the IDP used, fully unauthenticated attacks (e.g without access to a valid user) might also be feasible if generation of a signed message can be triggered. Users should upgrade to passport-saml version 3.2.2 or newer. The issue was also present in the beta releases of `node-saml` before version 4.0.0-beta.5. If you cannot upgrade, disabling SAML authentication may be done as a workaround. **CVE ID : CVE-2022-39299**	ac7e890a0c90bc7491ce33155e	
Vendor: pencidesign					
Product: soledad					
Affected Version(s): * Up to (excluding) 8.2.5					
Improper Neutralization of Input	10-Oct-2022	6.1	The soledad WordPress theme before 8.2.5 does not sanitise the	N/A	A-PEN-SOLE-201022/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			{id,datafilter[type],...} parameters in its penci_more_slist_post_ajax AJAX action, leading to a Reflected Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2022-3209**		
Vendor: Pfsense					
Product: pfsense					
Affected Version(s): 2.5.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Oct-2022	6.1	pfSense v2.5.2 was discovered to contain a cross-site scripting (XSS) vulnerability in the browser.php component. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into a file name. **CVE ID : CVE-2022-42247**	https://github.com/pfsense/pfsense/commit/73ca6743954ac9f35ca293e3f2af63eac20cf32e, https://gist.github.com/enferas/b4ca7a4fb52e1b5e698f87e4d655a70a	A-PFS-PFSE-201022/592
Vendor: Phpipam					
Product: phpipam					
Affected Version(s): 1.5.0					
Improper Encoding or Escaping of Output	03-Oct-2022	9.8	phpipam v1.5.0 was discovered to contain a header injection vulnerability via the component /admin/subnets/ripe-query.php.	N/A	A-PHP-PHPI-201022/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41443		
Vendor: picuploader_project					
Product: picuploader					
Affected Version(s): 2.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	6.1	PicUploader v2.6.3 was discovered to contain cross-site scripting (XSS) vulnerability via the setStorageParams function in SettingController.php. **CVE ID : CVE-2022-41442**	https://github.com/xiebruce/PicUploader/commit/2b0411bddb7942e0ace136a82d4ccde0fe66f263	A-PIC-PICU-201022/594
Vendor: pjsip					
Product: pjsip					
Affected Version(s): * Up to (excluding) 2.13					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	PJSIP is a free and open source multimedia communication library written in C. In versions of PJSIP prior to 2.13 the PJSIP parser, PJMEDIA RTP decoder, and PJMEDIA SDP parser are affeced by a buffer overflow vulnerability. Users connecting to untrusted clients are at risk. This issue has been patched and is available as commit	https://github.com/pjsip/pjproject/commit/c4d34984ec92b3d5252a7d5cddd85a1d3a8001ae, https://github.com/pjsip/pjproject/security/advisories/GHSA-fq45-m3f7-3mhj	A-PJS-PJSI-201022/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c4d3498 in the master branch and will be included in releases 2.13 and later. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39244**		
Affected Version(s): From (including) 2.11 Up to (excluding) 2.13					
Cleartext Transmission of Sensitive Information	06-Oct-2022	9.1	PJSIP is a free and open source multimedia communication library written in C. When processing certain packets, PJSIP may incorrectly switch from using SRTP media transport to using basic RTP upon SRTP restart, causing the media to be sent insecurely. The vulnerability impacts all PJSIP users that use SRTP. The patch is available as commit d2acb9a in the master branch of the project and will be included in version 2.13. Users are advised to manually patch or to upgrade. There are no known	https://github.com/pjsip/pjproject/commit/d2acb9af4e27b5ba75d658690406cec9c274c5cc, https://github.com/pjsip/pjproject/security/advisories/GHSA-wx5m-cj97-4wwg	A-PJS-PJSI-201022/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this vulnerability. **CVE ID : CVE-2022-39269**		
Vendor: Progress					
Product: whatsup_gold					
Affected Version(s): * Up to (excluding) 22.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Oct-2022	9.6	In Progress WhatsUp Gold before 22.1.0, an SNMP MIB Walker application endpoint failed to adequately sanitize malicious input. This could allow an unauthenticated attacker to execute arbitrary code in a victim's browser. **CVE ID : CVE-2022-42711**	https://www.progress.com/, https://community.progress.com/s/article/Product-Alert-Bulletin-October-2022, https://www.progress.com/network-monitoring	A-PRO-WHAT-201022/597
Vendor: projectworlds					
Product: online_examination_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Oct-2022	6.1	Online Examination System version 1.0 suffers from a cross site scripting vulnerability via index.php. **CVE ID : CVE-2022-42066**	N/A	A-PRO-ONLI-201022/598
Vendor: Puppet					
Product: puppetlabs-mysql					
Affected Version(s): * Up to (excluding) 13.0.0					
Improper Neutralizat	07-Oct-2022	8.8	Command injection is possible in the	https://puppet.com/security/c	A-PUP-PUPP-201022/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			puppetlabs-mysql module prior to version 13.0.0. A malicious actor is able to exploit this vulnerability only if they are able to provide unsanitized input to the module. This condition is rare in most deployments of Puppet and Puppet Enterprise. **CVE ID : CVE-2022-3276**	ve/CVE-2022-3276	
Affected Version(s): * Up to (excluding) 9.0.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Oct-2022	9.8	Command injection is possible in the puppetlabs-apt module prior to version 9.0.0. A malicious actor is able to exploit this vulnerability only if they are able to provide unsanitized input to the module. This condition is rare in most deployments of Puppet and Puppet Enterprise. **CVE ID : CVE-2022-3275**	https://puppet.com/security/cve/CVE-2022-3275	A-PUP-PUPP-201022/600
Vendor: puppycms					
Product: puppycms					
Affected Version(s): * Up to (including) 5.1					
Improper Neutralization of	12-Oct-2022	6.1	A vulnerability classified as problematic has	N/A	A-PUP-PUPP-201022/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			been found in puppyCMS up to 5.1. This affects an unknown part of the file /admin/settings.php. The manipulation of the argument site_name leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-210699. **CVE ID : CVE-2022-3464**		
Vendor: purchase_order_management_system_project					
Product: purchase_order_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Oct-2022	5.4	A vulnerability was found in SourceCodester Purchase Order Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the component Supplier Handler. The manipulation of the argument Supplier Name/Address/Contact person/Contact leads to cross site	N/A	A-PUR-PURC-201022/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210832. **CVE ID : CVE-2022-3503**		
Vendor: pyup					
Product: dependency_parser					
Affected Version(s): * Up to (excluding) 0.5.1					
Uncontrolled Resource Consumption	06-Oct-2022	7.5	dparse is a parser for Python dependency files. dparse in versions before 0.5.2 contain a regular expression that is vulnerable to a Regular Expression Denial of Service. All the users parsing index server URLs with dparse are impacted by this vulnerability. A patch has been applied in version `0.5.2`, all the users are advised to upgrade to `0.5.2` as soon as possible. Users unable to upgrade should avoid passing index server URLs in the	https://github.com/pyupio/dparse/commit/8c990170bbd6c0cf212f1151e9025486556062d5, https://github.com/pyupio/dparse/commit/d87364f9db9ab916451b1b036cfeb039e726e614, https://github.com/pyupio/dparse/security/advisories/GHSA-8fg9-p83m-x5pq	A-PYU-DEPE-201022/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			source file to be parsed. **CVE ID : CVE-2022-39280**		
Vendor: resiot					
Product: iot_platform_and_lorawan_network_server					
Affected Version(s): * Up to (excluding) 4.1.1000118					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Oct-2022	5.4	Multiple Cross Site Scripting (XSS) vulnerabilities in ResIOT IOT Platform + LoRaWAN Network Server through 4.1.1000114 via the form fields. **CVE ID : CVE-2022-34021**	https://securityblog101.blogspot.com/2022/09/cve-id-cve-2022-34021.html	A-RES-IOT_-201022/604
Affected Version(s): * Up to (including) 4.1.1000114					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.8	Cross Site Request Forgery (CSRF) vulnerability in ResIOT ResIOT IOT Platform + LoRaWAN Network Server through 4.1.1000114 allows attackers to add new admin users to the platform or other unspecified impacts. **CVE ID : CVE-2022-34020**	N/A	A-RES-IOT_-201022/605
Vendor: resmush.it					
Product: resmush.it_image_optimizer					
Affected Version(s): * Up to (excluding) 0.4.6					
Improper Neutralizat	10-Oct-2022	4.8	The reSmush.it WordPress plugin	N/A	A-RES-RESM-201022/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			before 0.4.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when unfiltered_html is disallowed. **CVE ID : CVE-2022-2448**		
Vendor: rpcms					
Product: rpcms					
Affected Version(s): 3.0.2					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.8	RPCMS v3.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily add an administrator account. **CVE ID : CVE-2022-41475**	N/A	A-RPC-RPCM-201022/607
Cross-Site Request Forgery (CSRF)	13-Oct-2022	6.5	RPCMS v3.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily change the password of any account. **CVE ID : CVE-2022-41474**	N/A	A-RPC-RPCM-201022/608
Improper Neutralizat	13-Oct-2022	6.1	RPCMS v3.0.2 was discovered to	N/A	A-RPC-RPCM-201022/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			contain a reflected cross-site scripting (XSS) vulnerability in the Search function. **CVE ID : CVE-2022-41473**		
Vendor: saleor					
Product: saleor					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 3.1.24					
Incorrect Authorization	06-Oct-2022	4.3	Saleor is a headless, GraphQL commerce platform. In affected versions some GraphQL mutations were not properly checking the ID type input which allowed to access database objects that the authenticated user may not be allowed to access. This vulnerability can be used to expose the following information: Estimating database row counts from tables with a sequential primary key or Exposing staff user and customer email addresses and full name through the `assignNavigation()` mutation. This issue has been patched in main and backported to	https://github.com/saleor/saleor/security/advisories/GHSA-xhq8-8c5v-w8ff, https://github.com/saleor/saleor/commit/96e04c092ddcac17b14f2e31554aa02d9006d0ce	A-SAL-SALE-201022/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple releases (3.7.17, 3.6.18, 3.5.23, 3.4.24, 3.3.26, 3.2.14, 3.1.24). Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39275**		
Affected Version(s): From (including) 3.2.0 Up to (excluding) 3.2.14					
Incorrect Authorization	06-Oct-2022	4.3	Saleor is a headless, GraphQL commerce platform. In affected versions some GraphQL mutations were not properly checking the ID type input which allowed to access database objects that the authenticated user may not be allowed to access. This vulnerability can be used to expose the following information: Estimating database row counts from tables with a sequential primary key or Exposing staff user and customer email addresses and full name through the `assignNavigation() ` mutation. This issue has been	https://github.com/saleor/saleor/security/advisories/GHSA-xhq8-8c5v-w8ff, https://github.com/saleor/saleor/commit/96e04c092ddcac17b14f2e31554aa02d9006d0ce	A-SAL-SALE-201022/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched in main and backported to multiple releases (3.7.17, 3.6.18, 3.5.23, 3.4.24, 3.3.26, 3.2.14, 3.1.24). Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39275**		
Affected Version(s): From (including) 3.3.0 Up to (excluding) 3.3.26					
Incorrect Authorization	06-Oct-2022	4.3	Saleor is a headless, GraphQL commerce platform. In affected versions some GraphQL mutations were not properly checking the ID type input which allowed to access database objects that the authenticated user may not be allowed to access. This vulnerability can be used to expose the following information: Estimating database row counts from tables with a sequential primary key or Exposing staff user and customer email addresses and full name through the `assignNavigation()	https://github.com/saleor/saleor/security/advisories/GHSA-xhq8-8c5v-w8ff, https://github.com/saleor/saleor/commit/96e04c092ddcac17b14f2e31554aa02d9006d0ce	A-SAL-SALE-201022/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			` mutation. This issue has been patched in main and backported to multiple releases (3.7.17, 3.6.18, 3.5.23, 3.4.24, 3.3.26, 3.2.14, 3.1.24). Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39275**		
Affected Version(s): From (including) 3.4.0 Up to (excluding) 3.4.24					
Incorrect Authorization	06-Oct-2022	4.3	Saleor is a headless, GraphQL commerce platform. In affected versions some GraphQL mutations were not properly checking the ID type input which allowed to access database objects that the authenticated user may not be allowed to access. This vulnerability can be used to expose the following information: Estimating database row counts from tables with a sequential primary key or Exposing staff user and customer email addresses and full	https://github.com/saleor/saleor/security/advisories/GHSA-xhq8-8c5v-w8ff, https://github.com/saleor/saleor/commit/96e04c092ddcac17b14f2e31554aa02d9006d0ce	A-SAL-SALE-201022/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name through the `assignNavigation()` mutation. This issue has been patched in main and backported to multiple releases (3.7.17, 3.6.18, 3.5.23, 3.4.24, 3.3.26, 3.2.14, 3.1.24). Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39275**		
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.23					
Incorrect Authorization	06-Oct-2022	4.3	Saleor is a headless, GraphQL commerce platform. In affected versions some GraphQL mutations were not properly checking the ID type input which allowed to access database objects that the authenticated user may not be allowed to access. This vulnerability can be used to expose the following information: Estimating database row counts from tables with a sequential primary key or Exposing staff user	https://github.com/saleor/saleor/security/advisories/GHSA-xhq8-8c5v-w8ff, https://github.com/saleor/saleor/commit/96e04c092ddcac17b14f2e31554aa02d9006d0ce	A-SAL-SALE-201022/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and customer email addresses and full name through the `assignNavigation()` mutation. This issue has been patched in main and backported to multiple releases (3.7.17, 3.6.18, 3.5.23, 3.4.24, 3.3.26, 3.2.14, 3.1.24). Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39275**		
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.18					
Incorrect Authorization	06-Oct-2022	4.3	Saleor is a headless, GraphQL commerce platform. In affected versions some GraphQL mutations were not properly checking the ID type input which allowed to access database objects that the authenticated user may not be allowed to access. This vulnerability can be used to expose the following information: Estimating database row counts from tables with a sequential	https://github.com/saleor/saleor/security/advisories/GHSA-xhq8-8c5v-w8ff, https://github.com/saleor/saleor/commit/96e04c092ddcac17b14f2e31554aa02d9006d0ce	A-SAL-SALE-201022/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			primary key or Exposing staff user and customer email addresses and full name through the `assignNavigation()` mutation. This issue has been patched in main and backported to multiple releases (3.7.17, 3.6.18, 3.5.23, 3.4.24, 3.3.26, 3.2.14, 3.1.24). Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39275**		
Affected Version(s): From (including) 3.7.0 Up to (excluding) 3.7.17					
Incorrect Authorization	06-Oct-2022	4.3	Saleor is a headless, GraphQL commerce platform. In affected versions some GraphQL mutations were not properly checking the ID type input which allowed to access database objects that the authenticated user may not be allowed to access. This vulnerability can be used to expose the following information: Estimating database row	https://github.com/saleor/saleor/security/advisories/GHSA-xhq8-8c5v-w8ff, https://github.com/saleor/saleor/commit/96e04c092ddcac17b14f2e31554aa02d9006d0ce	A-SAL-SALE-201022/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			counts from tables with a sequential primary key or Exposing staff user and customer email addresses and full name through the `assignNavigation() ` mutation. This issue has been patched in main and backported to multiple releases (3.7.17, 3.6.18, 3.5.23, 3.4.24, 3.3.26, 3.2.14, 3.1.24). Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39275**		
Vendor: Samsung					
Product: account					
Affected Version(s): * Up to (excluding) 13.5.01.3					
Insertion of Sensitive Information into Log File	07-Oct-2022	5.5	Sensitive log information leakage vulnerability in Samsung Account prior to version 13.5.0 allows attackers to unauthorized logout. **CVE ID : CVE-2022-39874**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-ACCO-201022/617
N/A	07-Oct-2022	4.7	Intent redirection vulnerability in Samsung Account	https://security.samsungmobile.com/service	A-SAM-ACCO-201022/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to version 13.5.01.3 allows attackers to access content providers without permission. **CVE ID : CVE-2022-39863**	Web.smsb?year=2022&month=10	
N/A	07-Oct-2022	4.4	Improper component protection vulnerability in Samsung Account prior to version 13.5.0 allows attackers to unauthorized logout. **CVE ID : CVE-2022-39875**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-ACCO-201022/619
Product: checkout					
Affected Version(s): * Up to (excluding) 5.0.55.3					
N/A	07-Oct-2022	5.5	Improper access control vulnerability in Samsung Checkout prior to version 5.0.55.3 allows attackers to access sensitive information via implicit intent broadcast. **CVE ID : CVE-2022-39878**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-CHEC-201022/620
Product: dynamic_lockscreen					
Affected Version(s): * Up to (excluding) 3.3.03.66					
Incorrect Authorization	07-Oct-2022	9.8	Improper authorization in Dynamic Lockscreen prior to	https://security.samsungmobile.com/serviceWeb.smsb?year	A-SAM-DYNA-201022/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMR Sep-2022 Release 1 in Android R(11) and 3.3.03.66 in Android S(12) allows unauthorized use of javascript interface api. **CVE ID : CVE-2022-39862**	=2022&month=10	
Product: factorycamera					
Affected Version(s): * Up to (excluding) 3.5.51					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Oct-2022	7.8	Path traversal vulnerability in AtBroadcastReceiver in FactoryCamera prior to version 3.5.51 allows attackers to write arbitrary file as FactoryCamera privilege. **CVE ID : CVE-2022-39858**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-FACT-201022/622
Missing Authorization	07-Oct-2022	3.3	Unprotected Receiver in AtBroadcastReceiver in FactoryCamera prior to version 3.5.51 allows attackers to record video without camera privilege. **CVE ID : CVE-2022-39861**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-FACT-201022/623
Product: factorycamerafb					
Affected Version(s): * Up to (excluding) 3.5.51					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	07-Oct-2022	5.5	Improper access control vulnerability in CameraTestActivity in FactoryCameraFB prior to version 3.5.51 allows attackers to access broadcasting Intent as system uid privilege. **CVE ID : CVE-2022-39857**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-FACT-201022/624
Product: group_sharing					
Affected Version(s): * Up to (excluding) 13.0.6.14					
Improper Privilege Management	07-Oct-2022	5.3	Improper access control vulnerability in ProfileSharingAccount in Group Sharing prior to versions 13.0.6.15 in Android S(12), 13.0.6.14 in Android R(11) and below allows attackers to identify the device. **CVE ID : CVE-2022-39877**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-GROU-201022/625
Affected Version(s): * Up to (excluding) 13.0.6.15					
Improper Privilege Management	07-Oct-2022	5.3	Improper access control vulnerability in ProfileSharingAccount in Group Sharing prior to versions 13.0.6.15 in Android S(12), 13.0.6.14 in Android R(11) and	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-GROU-201022/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below allows attackers to identify the device. **CVE ID : CVE-2022-39877**		
Product: internet					
Affected Version(s): * Up to (excluding) 18.0.4.14					
Incorrect Authorization	07-Oct-2022	4.6	Improper authorization vulnerability in Samsung Internet prior to version 18.0.4.14 allows physical attackers to add bookmarks in secret mode without user authentication. **CVE ID : CVE-2022-39873**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-INTE-201022/627
Product: quick_share					
Affected Version(s): * Up to (excluding) 13.2.3.5					
Exposure of Resource to Wrong Sphere	07-Oct-2022	3.5	Improper access control vulnerability in QuickShare prior to version 13.2.3.5 allows attackers to access sensitive information via implicit broadcast. **CVE ID : CVE-2022-39860**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-QUIC-201022/628
Product: reminder					
Affected Version(s): * Up to (excluding) 8.2.01.13					
Insertion of Sensitive Information into Log File	07-Oct-2022	3.3	Insertion of Sensitive Information into Log in PushRegIdUpdateCl	https://security.samsungmobile.com/serviceWeb.smsb?year	A-SAM-REMI-201022/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ient of SReminder prior to 8.2.01.13 allows attacker to access device IMEI. **CVE ID : CVE-2022-39876**	=2022&month=10	
Product: sharelive					
Affected Version(s): * Up to (excluding) 13.2.03.5					
Improper Handling of Exceptional Conditions	07-Oct-2022	3.3	Improper restriction of broadcasting Intent in ShareLive prior to version 13.2.03.5 leaks MAC address of the connected Bluetooth device. **CVE ID : CVE-2022-39872**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-SHAR-201022/630
Product: smartthings					
Affected Version(s): * Up to (excluding) 1.7.85.25					
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	Improper access control vulnerability in WifiSetupLaunchHelper in SmartThings prior to version 1.7.89.25 allows attackers to access sensitive information via implicit intent. **CVE ID : CVE-2022-39864**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-SMAR-201022/631
Affected Version(s): * Up to (excluding) 1.7.89.0					
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	Improper access control vulnerability in ContentsSharingActivity.java SmartThings prior	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-SMAR-201022/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to version 1.7.89.0 allows attackers to access sensitive information via implicit broadcast. **CVE ID : CVE-2022-39865**		
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	Improper access control vulnerability in RegisteredEventMediator.kt SmartThings prior to version 1.7.89.0 allows attackers to access sensitive information via implicit broadcast. **CVE ID : CVE-2022-39866**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-SMAR-201022/633
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	Improper access control vulnerability in cloudNotificationManager.java SmartThings prior to version 1.7.89.0 allows attackers to access sensitive information via SHOW_PERSISTENT_BANNER broadcast. **CVE ID : CVE-2022-39867**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-SMAR-201022/634
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	Improper access control vulnerability in GedSamsungAccount.kt SmartThings prior to version 1.7.89.0 allows	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-SMAR-201022/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to access sensitive information via implicit broadcast. **CVE ID : CVE-2022-39868**		
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	Improper access control vulnerability in cloudNotificationManager.java SmartThings prior to version 1.7.89.0 allows attackers to access sensitive information via REMOVE_PERSISTENT_BANNER broadcast. **CVE ID : CVE-2022-39869**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-SMAR-201022/636
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	Improper access control vulnerability in cloudNotificationManager.java SmartThings prior to version 1.7.89.0 allows attackers to access sensitive information via PUSH_MESSAGE_RECEIVED broadcast. **CVE ID : CVE-2022-39870**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-SMAR-201022/637
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	Improper access control vulnerability cloudNotificationManager.java in SmartThings prior to version 1.7.89.0	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-SMAR-201022/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to access sensitive information via implicit broadcasts. **CVE ID : CVE-2022-39871**		
Product: uphelper_library					
Affected Version(s): * Up to (excluding) 3.0.12					
N/A	07-Oct-2022	3.3	Implicit intent hijacking vulnerability in UPHelper library prior to version 3.0.12 allows attackers to access sensitive information via implicit intent. **CVE ID : CVE-2022-39859**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	A-SAM-UPHE-201022/639
Vendor: SAP					
Product: 3d_visual_enterprise_author					
Affected Version(s): 9.0					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated ACIS Part and Assembly (.sat, CoreCadTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-39803**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated SolidWorks Part (.sldprt, CoreCadTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-39804**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/641
Improper Restriction of Operations within the Bounds of	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Computer Graphics Metafile (.cgm,	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/	A-SAP-3D_V-201022/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			CgmTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-39805**	fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated SolidWorks Drawing (.slddrw, CoreCadTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwritten space in memory. **CVE ID : CVE-2022-39806**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Wavefront Object (.obj, ObjTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-39808**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/644
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated AutoCAD (.dwg, TeighaTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9,	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41167**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated CATIA5 Part (.catpart, CatiaTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41168**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated CATIA4 Part (.model, CatiaTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41170**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/647
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated AutoCAD (.dxf, TeighaTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41172**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Enhanced Metafile (.emf, emf.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41175**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/649
Improper Restriction of Operations within the Bounds of	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Iges Part and Assembly (.igs, .iges,	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/	A-SAP-3D_V-201022/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			CoreCadTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41177**	fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Jupiter Tesselation (.jt, JtTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwritten space in memory. **CVE ID : CVE-2022-41179**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Portable Document Format (.pdf, PDFPublishing.dll) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41180**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/652
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Windows Cursor File (.cur, ico.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41184**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Visual Design Stream (.vds, MataiPersistence.dll) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41185**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated SolidWorks Drawing (.sldasm, CoreCadTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-39807**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/655
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated Wavefront Object (.obj, ObjTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application.	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41166		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated CATIA5 Part (.catpart, CatiaTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-41169**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/657
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated CATIA4 Part (.model, CatiaTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user until restart of the application. **CVE ID : CVE-2022-41171**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated AutoCAD (.dxf, TeighaTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-41173**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/659
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated Right Hemisphere Material (.rhm, rh.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user until restart of the application. **CVE ID : CVE-2022-41174**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated Enhanced Metafile (.emf, emf.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-41176**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/661
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated Iges Part and Assembly (.igs, .iges, CoreCadTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user until restart of the application. **CVE ID : CVE-2022-41178**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated Portable Document Format (.pdf, PDFPublishing.dll) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-41181**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/663
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated Parasolid Part and Assembly (.x_b, CoreCadTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unavailable to the user until restart of the application. **CVE ID : CVE-2022-41182**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	5.5	Due to lack of proper memory management, when a victim opens manipulated Windows Cursor File (.cur, ico.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Author - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-41183**	https://launchpad.support.sap.com/#/notes/3245929, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/665
Product: 3d_visual_enterprise_viewer					
Affected Version(s): * Up to (excluding) 9.0					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens manipulated Computer Graphics Metafile (.cgm, CgmCore.dll) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, a Remote Code Execution can	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be triggered when payload forces a stack-based overflow and or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41186**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Wavefront Object (.obj, ObjTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41187**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/667
Improper Restriction of Operations within the	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens manipulated	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-3D_V-201022/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Wavefront Object (.obj, ObjTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-41188**	c68f7e60039b.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated AutoCAD (.dwg, TeighaTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41189**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated AutoCAD (.dxf, TeighaTranslator.exe) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41190**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/670
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Jupiter Tesselation (.jt, JTReader.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41191**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens manipulated Jupiter Tesselation (.jt, JTReader.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-41192**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/672
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Encapsulated Post Script (.eps, ai.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41193**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Encapsulated Postscript (.eps, ai.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-41194**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/674
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated EAAmiga Interchange File Format (.iff, 2d.x3d) file received from	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41195**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated VRML Worlds (.wrl, vrml.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41196		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated VRML Worlds (.wrl, vrml.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible for the application to crash and becomes temporarily unavailable to the user until restart of the application. **CVE ID : CVE-2022-41197**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/677
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated SketchUp (.skp, SketchUp.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41198**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Open Inventor File (.iv, vrml.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41199**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/679
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Scalable Vector Graphic (.svg, svg.x3d) file received from untrusted sources in SAP 3D Visual	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41200**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Right Hemisphere Binary (.rh, rh.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41201**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Oct-2022	7.8	Due to lack of proper memory management, when a victim opens a manipulated Visual Design Stream (.vds, vds.x3d) file received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9, it is possible that a Remote Code Execution can be triggered when payload forces a stack-based overflow or a re-use of dangling pointer which refers to overwritten space in memory. **CVE ID : CVE-2022-41202**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-201022/682
Product: businessobjects_business_intelligence					
Affected Version(s): 420					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	SAP BusinessObjects BI LaunchPad - versions 420, 430, is susceptible to script execution attack by an unauthenticated attacker due to improper sanitization of the user inputs while interacting on the network. On successful	https://launchpad.support.sap.com/#/notes/3211161, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-201022/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2022-39800**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	SAP BusinessObjects Business Intelligence platform (Analysis for OLAP) - versions 420, 430, allows an authenticated attacker to send user-controlled inputs when OLAP connections are created and edited in the Central Management Console. On successful exploitation, there could be a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2022-41206**	https://launchpad.support.sap.com/#/notes/3229425, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-201022/684
Exposure of Sensitive Information to an	11-Oct-2022	4.9	Under certain conditions, the application SAP BusinessObjects Business Intelligence	https://launchpad.support.sap.com/#/notes/3233226, https://www.sap.com/docum	A-SAP-BUSI-201022/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Platform (Version Management System) exposes sensitive information to an actor over the network with high privileges that is not explicitly authorized to have access to that information, leading to a high impact on Confidentiality. **CVE ID : CVE-2022-35296**	ents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 430					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	SAP BusinessObjects BI LaunchPad - versions 420, 430, is susceptible to script execution attack by an unauthenticated attacker due to improper sanitization of the user inputs while interacting on the network. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	https://launchpad.support.sap.com/#/notes/3211161, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-201022/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39800		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	SAP BusinessObjects Business Intelligence platform (Analysis for OLAP) - versions 420, 430, allows an authenticated attacker to send user-controlled inputs when OLAP connections are created and edited in the Central Management Console. On successful exploitation, there could be a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2022-41206**	https://launchpad.support.sap.com/#/notes/3229425, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-201022/687
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	4.9	Under certain conditions, the application SAP BusinessObjects Business Intelligence Platform (Version Management System) exposes sensitive information to an actor over the network with high privileges that is not explicitly	https://launchpad.support.sap.com/#/notes/3233226, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-201022/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorized to have access to that information, leading to a high impact on Confidentiality. **CVE ID : CVE-2022-35296**		
Product: business_objects_business_intelligence_platform					
Affected Version(s): 420					
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	7.6	Under certain conditions an authenticated attacker can get access to OS credentials. Getting access to OS credentials enables the attacker to modify system data and make the system unavailable leading to high impact on confidentiality and low impact on integrity and availability of the application. **CVE ID : CVE-2022-39013**	https://launchpad.support.sap.com/#/notes/3229132, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-201022/689
Exposure of Resource to Wrong Sphere	11-Oct-2022	6.5	Under certain conditions, BOE AdminTools/ BOE SDK allows an attacker to access information which would otherwise be restricted. **CVE ID : CVE-2022-39015**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-201022/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 430					
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	7.6	Under certain conditions an authenticated attacker can get access to OS credentials. Getting access to OS credentials enables the attacker to modify system data and make the system unavailable leading to high impact on confidentiality and low impact on integrity and availability of the application. **CVE ID : CVE-2022-39013**	https://launchpad.support.sap.com/#/notes/3229132, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-201022/691
Exposure of Resource to Wrong Sphere	11-Oct-2022	6.5	Under certain conditions, BOE AdminTools/ BOE SDK allows an attacker to access information which would otherwise be restricted. **CVE ID : CVE-2022-39015**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-201022/692
Product: commerce					
Affected Version(s): 1905					
URL Redirection to Untrusted Site ('Open Redirect')	11-Oct-2022	8.8	An attacker can change the content of an SAP Commerce - versions 1905, 2005, 2105, 2011, 2205, login page through a	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launch	A-SAP-COMM-201022/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulated URL. They can inject code that allows them to redirect submissions from the affected login form to their own server. This allows them to steal credentials and hijack accounts. A successful attack could compromise the Confidentiality, Integrity, and Availability of the system. **CVE ID : CVE-2022-41204**	pad.support.sap.com/#/notes/3239152	
Affected Version(s): 2005					
URL Redirection to Untrusted Site ('Open Redirect')	11-Oct-2022	8.8	An attacker can change the content of an SAP Commerce - versions 1905, 2005, 2105, 2011, 2205, login page through a manipulated URL. They can inject code that allows them to redirect submissions from the affected login form to their own server. This allows them to steal credentials and hijack accounts. A successful attack could compromise the Confidentiality, Integrity, and	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3239152	A-SAP-COMM-201022/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Availability of the system. **CVE ID : CVE-2022-41204**		
Affected Version(s): 2011					
URL Redirection to Untrusted Site ('Open Redirect')	11-Oct-2022	8.8	An attacker can change the content of an SAP Commerce - versions 1905, 2005, 2105, 2011, 2205, login page through a manipulated URL. They can inject code that allows them to redirect submissions from the affected login form to their own server. This allows them to steal credentials and hijack accounts. A successful attack could compromise the Confidentiality, Integrity, and Availability of the system. **CVE ID : CVE-2022-41204**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3239152	A-SAP-COMM-201022/695
Affected Version(s): 2105					
URL Redirection to Untrusted Site ('Open Redirect')	11-Oct-2022	8.8	An attacker can change the content of an SAP Commerce - versions 1905, 2005, 2105, 2011, 2205, login page through a manipulated URL.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sa	A-SAP-COMM-201022/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			They can inject code that allows them to redirect submissions from the affected login form to their own server. This allows them to steal credentials and hijack accounts. A successful attack could compromise the Confidentiality, Integrity, and Availability of the system. **CVE ID : CVE-2022-41204**	p.com/#/notes/3239152	
Affected Version(s): 2205					
URL Redirection to Untrusted Site ('Open Redirect')	11-Oct-2022	8.8	An attacker can change the content of an SAP Commerce - versions 1905, 2005, 2105, 2011, 2205, login page through a manipulated URL. They can inject code that allows them to redirect submissions from the affected login form to their own server. This allows them to steal credentials and hijack accounts. A successful attack could compromise the Confidentiality, Integrity, and	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3239152	A-SAP-COMM-201022/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Availability of the system. **CVE ID : CVE-2022-41204**		
Product: customer_data_cloud					
Affected Version(s): 7.4					
Inadequate Encryption Strength	11-Oct-2022	5.2	SAP Customer Data Cloud (Gigya mobile app for Android) - version 7.4, uses encryption method which lacks proper diffusion and does not hide the patterns well. This can lead to information disclosure. In certain scenarios, application might also be susceptible to replay attacks. **CVE ID : CVE-2022-41209**	https://launchpad.support.sap.com/#/notes/3248970, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-201022/698
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	11-Oct-2022	5.2	SAP Customer Data Cloud (Gigya mobile app for Android) - version 7.4, uses insecure random number generator program which makes it easy for the attacker to predict future random numbers. This can lead to information disclosure and modification of certain user settings.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3248384	A-SAP-CUST-201022/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41210		
Product: data_services					
Affected Version(s): 4.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	SAP Data Services Management allows an attacker to copy the data from a request and echoed into the application's immediate response, it will lead to a Cross-Site Scripting vulnerability. The attacker would have to log in to the management console to perform such as an attack, only few of the pages are vulnerable in the DS management console. **CVE ID : CVE-2022-35226**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3167342	A-SAP-DATA-201022/700
Affected Version(s): 4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	SAP Data Services Management allows an attacker to copy the data from a request and echoed into the application's immediate response, it will lead to a Cross-Site Scripting vulnerability. The attacker would	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3167342	A-SAP-DATA-201022/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have to log in to the management console to perform such as an attack, only few of the pages are vulnerable in the DS management console. **CVE ID : CVE-2022-35226**		
Product: enable_now					
Affected Version(s): 10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	The application SAP Enable Now does not sufficiently encode user-controlled inputs over the network before it is placed in the output being served to other users, thereby expanding the attack scope, resulting in Stored Cross-Site Scripting (XSS) vulnerability leading to limited impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2022-35297**	https://launchpad.support.sap.com/#/notes/3049899, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENAB-201022/702
Product: manufacturing_execution					
Affected Version(s): 15.1					
Improper Limitation of a Pathname	11-Oct-2022	7.5	SAP Manufacturing Execution - versions 15.1, 15.2, 15.3, allows an	https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-MANU-201022/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			attacker to exploit insufficient validation of a file path request parameter. The intended file path can be manipulated to allow arbitrary traversal of directories on the remote server. The file content within each directory can be read which may lead to information disclosure. **CVE ID : CVE-2022-39802**	0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3242933,https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 15.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Oct-2022	7.5	SAP Manufacturing Execution - versions 15.1, 15.2, 15.3, allows an attacker to exploit insufficient validation of a file path request parameter. The intended file path can be manipulated to allow arbitrary traversal of directories on the remote server. The file content within each directory can be read which may lead to information disclosure. **CVE ID : CVE-2022-39802**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3242933,https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MANU-201022/704
Affected Version(s): 15.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Oct-2022	7.5	SAP Manufacturing Execution - versions 15.1, 15.2, 15.3, allows an attacker to exploit insufficient validation of a file path request parameter. The intended file path can be manipulated to allow arbitrary traversal of directories on the remote server. The file content within each directory can be read which may lead to information disclosure. **CVE ID : CVE-2022-39802**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3242933,https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MANU-201022/705
Product: sap_iq					
Affected Version(s): 16.1					
Stack-based Buffer Overflow	11-Oct-2022	9.8	SAP SQL Anywhere - version 17.0, and SAP IQ - version 16.1, allows an attacker to leverage logical errors in memory management to cause a memory corruption, such as Stack-based buffer overflow. **CVE ID : CVE-2022-35299**	https://launchpad.support.sap.com/#/notes/3232021, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SAP_-201022/706
Product: sql_anywhere					
Affected Version(s): 17.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	11-Oct-2022	9.8	SAP SQL Anywhere - version 17.0, and SAP IQ - version 16.1, allows an attacker to leverage logical errors in memory management to cause a memory corruption, such as Stack-based buffer overflow. **CVE ID : CVE-2022-35299**	https://launchpad.support.sap.com/#/notes/3232021, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SQL_-201022/707
Vendor: semtech					
Product: loramac-node					
Affected Version(s): * Up to (excluding) 4.7.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	LoRaMac-node is a reference implementation and documentation of a LoRa network node. Versions of LoRaMac-node prior to 4.7.0 are vulnerable to a buffer overflow. Improper size validation of the incoming radio frames can lead to an 65280-byte out-of-bounds write. The function `ProcessRadioRxDone` implicitly expects incoming radio frames to have at least a payload of one byte or more. An empty payload leads to a	https://github.com/Lora-net/LoRaMac-node/commit/e851b079c82ba1bcf3f4d291ab69a571b0bf458a, https://github.com/Lora-net/LoRaMac-node/security/advisories/GHSA-7vv8-73pc-63c2	A-SEM-LORA-201022/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1-byte out-of-bounds read of user controlled content when the payload buffer is reused. This allows an attacker to craft a FRAME_TYPE_PROPRIETARY frame with size -1 which results in an 65280-byte out-of-bounds memcopy likely with partially controlled attacker data. Corrupting a large part if the data section is likely to cause a DoS. If the large out-of-bounds write does not immediately crash the attacker may gain control over the execution due to now controlling large parts of the data section. Users are advised to upgrade either by updating their package or by manually applying the patch commit `e851b079`. **CVE ID : CVE-2022-39274**		
Vendor: shortpixel					
Product: enable_media_replace					
Affected Version(s): * Up to (excluding) 4.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Oct-2022	4.9	The Enable Media Replace WordPress plugin before 4.0.0 does not ensure that renamed files are moved to the Upload folder, which could allow high privilege users such as admin to move them outside to the web root directory via a path traversal attack for example **CVE ID : CVE-2022-2554**	N/A	A-SHO-ENAB-201022/709
Vendor: Siemens					
Product: industrial_edge_management					
Affected Version(s): * Up to (excluding) 1.5.1					
Improper Certificate Validation	11-Oct-2022	7.4	A vulnerability has been identified in Industrial Edge Management (All versions < V1.5.1). The affected software does not properly validate the server certificate when initiating a TLS connection. This could allow an attacker to spoof a trusted entity by interfering in the communication path between the client and the intended server. **CVE ID : CVE-2022-40147**	https://cert-portal.siemens.com/productcert/pdf/ssa-649853.pdf	A-SIE-INDU-201022/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: jt_open_toolkit					
Affected Version(s): * Up to (excluding) 11.1.1.0					
Access of Uninitialized Pointer	11-Oct-2022	7.8	A vulnerability has been identified in JTTK (All versions < V11.1.1.0), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The JTTK library is vulnerable to an uninitialized pointer reference vulnerability while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-16973) **CVE ID : CVE-2022-41851**	https://cert-portal.siemens.com/productcert/pdf/ssa-611756.pdf	A-SIE-JT_O-201022/711
Product: nucleus_net					
Affected Version(s): *					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	A-SIE-NUCL-201022/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: nucleus_readystart_v3					
Affected Version(s): *					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	A-SIE-NUCL-201022/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: nucleus_source_code					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	A-SIE-NUCL-201022/714
Product: simatic_s7-1500_software_controller					
Affected Version(s): * Up to (excluding) 21.9					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family	https://cert-portal.siemens.com/productce	A-SIE-SIMA-201022/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simcenter_femap					
Affected Version(s): From (including) 2022.1.0 Up to (excluding) 2022.1.3					
Access of Uninitialized Pointer	11-Oct-2022	7.8	A vulnerability has been identified in JTTK (All versions < V11.1.1.0), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The JTTK library is vulnerable to an uninitialized pointer reference vulnerability while parsing specially	https://cert-portal.siemens.com/productcert/pdf/ssa-611756.pdf	A-SIE-SIMC-201022/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-16973) **CVE ID : CVE-2022-41851**		
Affected Version(s): From (including) 2022.2.0 Up to (excluding) 2022.2.2					
Access of Uninitialized Pointer	11-Oct-2022	7.8	A vulnerability has been identified in JTTK (All versions < V11.1.1.0), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The JTTK library is vulnerable to an uninitialized pointer reference vulnerability while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-16973) **CVE ID : CVE-2022-41851**	https://cert-portal.siemens.com/productcert/pdf/ssa-611756.pdf	A-SIE-SIMC-201022/717
Product: solid_edge					
Affected Version(s): se2020					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	11-Oct-2022	7.8	A vulnerability has been identified in Solid Edge (All Versions < SE2022MP9). The affected application contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted DWG files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17627) **CVE ID : CVE-2022-37864**	https://cert-portal.siemens.com/productcert/pdf/ssa-258115.pdf	A-SIE-SOLI-201022/718
Vendor: simplefilelist					
Product: simple-file-list					
Affected Version(s): * Up to (excluding) 4.4.12					
Cross-Site Request Forgery (CSRF)	10-Oct-2022	6.5	The Simple File List WordPress plugin before 4.4.12 does not implement nonce checks, which could allow attackers to make a logged in admin create new page and change it's content via a CSRF attack. **CVE ID : CVE-2022-3208**	N/A	A-SIM-SIMP-201022/719
Improper Neutralization of Input	10-Oct-2022	4.8	The Simple File List WordPress plugin before 4.4.12 does not sanitise and	N/A	A-SIM-SIMP-201022/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-3207**		
Vendor: simple_cold_storage_management_system_project					
Product: simple_cold_storage_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-2022	7.2	Simple Cold Storage Management System v1.0 is vulnerable to SQL injection via /csms/classes/Master.php?f=delete_message. **CVE ID : CVE-2022-42241**	N/A	A-SIM-SIMP-201022/721
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-2022	7.2	Simple Cold Storage Management System v1.0 is vulnerable to SQL injection via /csms/classes/Master.php?f=delete_booking. **CVE ID : CVE-2022-42242**	N/A	A-SIM-SIMP-201022/722
Improper Neutralization of	06-Oct-2022	7.2	Simple Cold Storage Management System v1.0 is	N/A	A-SIM-SIMP-201022/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			vulnerable to SQL injection via /csms/admin/storages/manage_storage.php?id=. **CVE ID : CVE-2022-42243**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-2022	7.2	Simple Cold Storage Management System v1.0 is vulnerable to SQL injection via /csms/admin/storages/view_storage.php?id=. **CVE ID : CVE-2022-42249**	N/A	A-SIM-SIMP-201022/724
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-2022	7.2	Simple Cold Storage Management System v1.0 is vulnerable to SQL injection via /csms/admin/inquiries/view_details.php?id=. **CVE ID : CVE-2022-42250**	N/A	A-SIM-SIMP-201022/725
Product: simple_cold_storage_managment_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Oct-2022	7.2	Simple Cold Storage Management System v1.0 is vulnerable to SQL Injection via /csms/admin/?page=user/manage_user&id=. **CVE ID : CVE-2022-42230**	N/A	A-SIM-SIMP-201022/726
Vendor: simple_e-learning_system_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: simple_e-learning_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	An SQL injection vulnerability issue was discovered in Sourcecodester Simple E-Learning System 1.0., in /vcs/classRoom.php?classCode=, classCode. **CVE ID : CVE-2022-40872**	N/A	A-SIM-SIMP-201022/727
Vendor: simple_online_public_access_catalog_project					
Product: simple_online_public_access_catalog					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Oct-2022	7.2	A vulnerability has been found in SourceCodester Simple Online Public Access Catalog 1.0 and classified as critical. This vulnerability affects unknown code of the file /opac/Actions.php?a=login of the component Admin Login. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this	N/A	A-SIM-SIMP-201022/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-210784. **CVE ID : CVE-2022-3495**		
Vendor: slack_morphism_project					
Product: slack_morphism					
Affected Version(s): * Up to (including) 1.3.0					
Exposure of Sensitive System Information Due to Uncleared Debug Information	10-Oct-2022	7.5	Slack Morphism is a modern client library for Slack Web/Events API/Socket Mode and Block Kit. Debug logs expose sensitive URLs for Slack webhooks that contain private information. The problem is fixed in version 1.3.2 which redacts sensitive URLs for webhooks. As a workaround, people who use Slack webhooks may disable or filter debug logs. **CVE ID : CVE-2022-39292**	https://github.com/abdolence/slack-morphism-rust/security/advisories/GHSA-4mjx-2gh5-ph8h	A-SLA-SLAC-201022/729
Vendor: snyk					
Product: cli					
Affected Version(s): * Up to (excluding) 1.996.0					
Improper Neutralization of Special Elements used in a Command ('Comman	03-Oct-2022	7.8	Snyk CLI before 1.996.0 allows arbitrary command execution, affecting Snyk IDE plugins and the snyk npm package. Exploitation could follow from the	https://github.com/snyk/snyk-go-plugin/releases/tag/v1.19.1, https://github.com/snyk/cli/r	A-SNY-CLI-201022/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			common practice of viewing untrusted files in the Visual Studio Code editor, for example. The original demonstration was with shell metacharacters in the vendor.json ignore field, affecting snyk-go-plugin before 1.19.1. This affects, for example, the Snyk TeamCity plugin (which does not update automatically) before 20220930.142957. **CVE ID : CVE-2022-40764**	eleases/tag/v1.996.0	
Product: golang_cli					
Affected Version(s): * Up to (excluding) 1.19.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Oct-2022	7.8	Snyk CLI before 1.996.0 allows arbitrary command execution, affecting Snyk IDE plugins and the snyk npm package. Exploitation could follow from the common practice of viewing untrusted files in the Visual Studio Code editor, for example. The original demonstration was with shell metacharacters in	https://github.com/snyk/snyk-go-plugin/releases/tag/v1.19.1, https://github.com/snyk/cli/releases/tag/v1.996.0	A-SNY-GOLA-201022/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the vendor.json ignore field, affecting snyk-go-plugin before 1.19.1. This affects, for example, the Snyk TeamCity plugin (which does not update automatically) before 20220930.142957. **CVE ID : CVE-2022-40764**		
Vendor: sonicjs					
Product: sonicjs					
Affected Version(s): * Up to (including) 0.6.0					
Out-of-bounds Write	01-Oct-2022	9.1	SonicJS through 0.6.0 allows file overwrite. It has the following mutations that are used for updating files: fileCreate and fileUpdate. Both of these mutations can be called without any authentication to overwrite any files on a SonicJS application, leading to Arbitrary File Write and Delete. **CVE ID : CVE-2022-42002**	N/A	A-SON-SONI-201022/732
Vendor: student_clearance_system_project					
Product: student_clearance_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A Stored XSS issue in Student Clearance System v.1.0 allows the injection of arbitrary JavaScript in the Student registration form. **CVE ID : CVE-2022-42235**	N/A	A-STU-STUD-201022/733
Vendor: Swftools					
Product: swftools					
Affected Version(s): 2021-12-16					
Out-of-bounds Write	13-Oct-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via png_load at /lib/png.c. **CVE ID : CVE-2022-35080**	N/A	A-SWF-SWFT-201022/734
Out-of-bounds Write	13-Oct-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via png_read_header at /src/png2swf.c. **CVE ID : CVE-2022-35081**	N/A	A-SWF-SWFT-201022/735
Vendor: sylabs					
Product: singularity_image_format					
Affected Version(s): * Up to (excluding) 2.8.1					
Improper Verification of Cryptographic Signature	06-Oct-2022	9.8	syslabs/sif is the Singularity Image Format (SIF) reference implementation. In versions prior to	https://github.com/sylabs/sif/security/advisories/GHSA-m5m3-46gj-wch8,	A-SYL-SING-201022/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.8.1the `github.com/sylabs/sif/v2/pkg/integrity` package did not verify that the hash algorithm(s) used are cryptographically secure when verifying digital signatures. A patch is available in version >= v2.8.1 of the module. Users are encouraged to upgrade. Users unable to upgrade may independently validate that the hash algorithm(s) used for metadata digest(s) and signature hash are cryptographically secure. **CVE ID : CVE-2022-39237**	https://github.com/sylabs/sif/commit/07fb86029a12e3210f6131e065570124605daeaa	
Vendor: taskbuilder					
Product: taskbuilder					
Affected Version(s): * Up to (excluding) 1.0.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2022	5.4	The Taskbuilder WordPress plugin before 1.0.8 does not validate and sanitise task's attachments, which could allow any authenticated user (such as subscriber) creating a task to perform Stored	N/A	A-TAS-TASK-201022/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting by attaching a malicious SVG file **CVE ID : CVE-2022-3137**		
Vendor: tiny-csrf_project					
Product: tiny-csrf					
Affected Version(s): * Up to (excluding) 1.1.0					
Cleartext Transmission of Sensitive Information	07-Oct-2022	6.5	tiny-csrf is a Node.js cross site request forgery (CSRF) protection middleware. In versions prior to 1.1.0 cookies were not encrypted and thus CSRF tokens were transmitted in the clear. This issue has been addressed in commit `8eead6d` and the patch with be included in version 1.1.0. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39287**	https://github.com/valexandersaulys/tiny-csrf/security/advisories/GHSA-pj2c-h76w-vv6f, https://github.com/valexandersaulys/tiny-csrf/commit/8eead6da3b56e290512bbe8d20c2c5df3be317ba	A-TIN-TINY-201022/738
Vendor: tooljet					
Product: tooljet					
Affected Version(s): * Up to (excluding) 1.26.1					
Improper Privilege Management	07-Oct-2022	7.5	Account Takeover :: when see the info i can see the hash pass i can creaked it ..... Account Takeover :: when	https://huntr.dev/bounties/02da53ab-f613-4171-8766-96b31c671551, https://github.	A-TOO-TOOL-201022/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see the info i can see the forgot_password_token the hacker can send the request and changed the pass **CVE ID : CVE-2022-3422**	com/tooljet/tooljet/commit/7879d8a76000c014533a97a22bc276afe3ae3e54	
Vendor: totaljs					
Product: total.js					
Affected Version(s): 2022-08-20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	5.4	A cross-site scripting (XSS) vulnerability in TotalJS commit 8c2c8909 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Website name text field under Main Settings. **CVE ID : CVE-2022-41392**	N/A	A-TOT-TOTA-201022/740
Vendor: traefik					
Product: traefik					
Affected Version(s): * Up to (excluding) 2.8.8					
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Traefik (pronounced traffic) is a modern HTTP reverse proxy and load balancer that assists in deploying microservices. There is a potential vulnerability in Traefik managing	https://github.com/traefik/traefik/security/advisories/GHSA-c6hx-pjc3-7fqr	A-TRA-TRAE-201022/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP/2 connections. A closing HTTP/2 server connection could hang forever because of a subsequent fatal error. This failure mode could be exploited to cause a denial of service. There has been a patch released in versions 2.8.8 and 2.9.0-rc5. There are currently no known workarounds. **CVE ID : CVE-2022-39271**		
Affected Version(s): 2.9.0					
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Traefik (pronounced traffic) is a modern HTTP reverse proxy and load balancer that assists in deploying microservices. There is a potential vulnerability in Traefik managing HTTP/2 connections. A closing HTTP/2 server connection could hang forever because of a subsequent fatal error. This failure mode could be exploited to cause a denial of service. There has been a	https://github.com/traefik/traefik/security/advisories/GHSA-c6hx-pjc3-7fqr	A-TRA-TRAE-201022/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patch released in versions 2.8.8 and 2.9.0-rc5. There are currently no known workarounds. **CVE ID : CVE-2022-39271**		
Vendor: Trendmicro					
Product: apex_one					
Affected Version(s): 2019					
Direct Request ('Forced Browsing')	10-Oct-2022	9.1	A forced browsing vulnerability in Trend Micro Apex One could allow an attacker with access to the Apex One console on affected installations to escalate privileges and modify certain agent groupings. Please note: an attacker must first obtain the ability to log onto the Apex One web console in order to exploit this vulnerability. **CVE ID : CVE-2022-41746**	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/743
Improper Certificate Validation	10-Oct-2022	7.8	An improper certification validation vulnerability in Trend Micro Apex One agents could allow a local attacker to load a DLL file with system service privileges on	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41747**		
Origin Validation Error	10-Oct-2022	7.8	An origin validation error vulnerability in Trend Micro Apex One agents could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41749**	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/745
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2022	7	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One Vulnerability Protection integrated component could allow a local attacker to escalate privileges and turn a specific working	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory into a mount point on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41744**		
Out-of-bounds Read	10-Oct-2022	7	An Out-of-Bounds access vulnerability in Trend Micro Apex One could allow a local attacker to create a specially crafted message to cause memory corruption on a certain service process which could lead to local privilege escalation on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41745**	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/747
Incorrect Default	10-Oct-2022	6.7	A registry permissions vulnerability in the Trend Micro Apex	https://success.trendmicro.co	A-TRE-APEX-201022/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			One Data Loss Prevention (DLP) module could allow a local attacker with administrative credentials to bypass certain elements of the product's anti-tampering mechanisms on affected installations. Please note: an attacker must first obtain administrative credentials on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41748**	m/solution/000291645	
Affected Version(s): -					
Direct Request ('Forced Browsing')	10-Oct-2022	9.1	A forced browsing vulnerability in Trend Micro Apex One could allow an attacker with access to the Apex One console on affected installations to escalate privileges and modify certain agent groupings. Please note: an attacker must first obtain the ability to log onto the Apex One web console in order to exploit this vulnerability.	https://success.trendmicro.com/solution/000291645	A-TRE-APEX-201022/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41746		
Improper Certificate Validation	10-Oct-2022	7.8	An improper certification validation vulnerability in Trend Micro Apex One agents could allow a local attacker to load a DLL file with system service privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41747**	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/750
Origin Validation Error	10-Oct-2022	7.8	An origin validation error vulnerability in Trend Micro Apex One agents could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41749		
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2022	7	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One Vulnerability Protection integrated component could allow a local attacker to escalate privileges and turn a specific working directory into a mount point on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41744**	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/752
Out-of-bounds Read	10-Oct-2022	7	An Out-of-Bounds access vulnerability in Trend Micro Apex One could allow a local attacker to create a specially crafted message to cause memory corruption on a certain service process which could lead to local privilege escalation on affected installations. Please	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41745**		
Incorrect Default Permissions	10-Oct-2022	6.7	A registry permissions vulnerability in the Trend Micro Apex One Data Loss Prevention (DLP) module could allow a local attacker with administrative credentials to bypass certain elements of the product's anti-tampering mechanisms on affected installations. Please note: an attacker must first obtain administrative credentials on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41748**	https://success.trendmicro.com/solution/0000291645	A-TRE-APEX-201022/754
Vendor: vanderbilt					
Product: redcap					
Affected Version(s): * Up to (excluding) 12.4.18					
Improper Neutralization of	12-Oct-2022	6.1	A reflected XSS vulnerability exists in REDCap before	N/A	A-VAN-REDC-201022/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			12.04.18 in the Alerts & Notifications upload feature. A crafted CSV file will, when uploaded, trigger arbitrary JavaScript code execution. **CVE ID : CVE-2022-42715**		
Affected Version(s): From (including) 12.5.0 Up to (excluding) 12.5.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Oct-2022	6.1	A reflected XSS vulnerability exists in REDCap before 12.04.18 in the Alerts & Notifications upload feature. A crafted CSV file will, when uploaded, trigger arbitrary JavaScript code execution. **CVE ID : CVE-2022-42715**	N/A	A-VAN-REDC-201022/756
Vendor: Veritas					
Product: netbackup					
Affected Version(s): * Up to (including) 10.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Oct-2022	9.8	An issue was discovered in Veritas NetBackup through 10.0 and related Veritas products. The NetBackup Primary server is vulnerable to a SQL Injection attack affecting the NBFSMCLIENT service.	https://www.veritas.com/content/support/en_US/security/VTS22-011#C1	A-VER-NETB-201022/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42302		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Oct-2022	9.8	An issue was discovered in Veritas NetBackup through 10.0 and related Veritas products. The NetBackup Primary server is vulnerable to a second-order SQL Injection attack affecting the NBFSMCLIENT service by leveraging CVE-2022-42302. **CVE ID : CVE-2022-42303**	https://www.veritas.com/content/support/en_US/security/VTS22-011#H1	A-VER-NETB-201022/758
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Oct-2022	9.8	An issue was discovered in Veritas NetBackup through 10.0 and related Veritas products. The NetBackup Primary server is vulnerable to a SQL Injection attack affecting idm, nbars, and SLP manager code. **CVE ID : CVE-2022-42304**	https://www.veritas.com/content/support/en_US/security/VTS22-011#H2	A-VER-NETB-201022/759
Affected Version(s): * Up to (including) 10.0.0.1					
Improper Restriction of XML External Entity Reference	03-Oct-2022	9.8	An issue was discovered in Veritas NetBackup through 10.0.0.1 and related Veritas products. The NetBackup Primary server is vulnerable	https://www.veritas.com/content/support/en_US/security/VTS22-012#M2	A-VER-NETB-201022/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to an XML External Entity (XXE) Injection attack through the DiscoveryService service. **CVE ID : CVE-2022-42307**		
Improper Restriction of XML External Entity Reference	03-Oct-2022	8.8	An issue was discovered in Veritas NetBackup through 10.0.0.1 and related Veritas products. The NetBackup Primary server is vulnerable to an XML External Entity (XXE) injection attack through the nbars process. **CVE ID : CVE-2022-42301**	https://www.veritas.com/content/support/en_US/security/VTS22-013#M1	A-VER-NETB-201022/761
N/A	03-Oct-2022	7.5	An issue was discovered in Veritas NetBackup through 10.0.0.1 and related Veritas products. The NetBackup Primary server is vulnerable to a denial of service attack through the DiscoveryService service. **CVE ID : CVE-2022-42299**	https://www.veritas.com/content/support/en_US/security/VTS22-012#M3	A-VER-NETB-201022/762
Improper Limitation of a Pathname	03-Oct-2022	7.5	An issue was discovered in Veritas NetBackup through 10.0.0.1	https://www.veritas.com/content/support/en	A-VER-NETB-201022/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			and related Veritas products. The NetBackup Primary server is vulnerable to a Path traversal attack through the DiscoveryService service. **CVE ID : CVE-2022-42305**	_US/security/VTS22-012#M1	
N/A	03-Oct-2022	6.5	An issue was discovered in Veritas NetBackup through 10.0.0.1 and related Veritas products. The NetBackup Primary server nbars process can be crashed resulting in a denial of service. (Note: the watchdog service will automatically restart the process.) **CVE ID : CVE-2022-42300**	https://www.veritas.com/content/support/en_US/security/VTS22-013#M2	A-VER-NETB-201022/764
Affected Version(s): * Up to (including) 8.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Oct-2022	7.1	An issue was discovered in Veritas NetBackup through 8.2 and related Veritas products. An attacker with local access can delete arbitrary files by leveraging a path traversal in the pbx_exchange registration code.	https://www.veritas.com/content/support/en_US/security/VTS22-010#C1	A-VER-NETB-201022/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42308		
NULL Pointer Dereference	03-Oct-2022	5.5	An issue was discovered in Veritas NetBackup through 8.2 and related Veritas products. An attacker with local access can send a crafted packet to pbx_exchange during registration and cause a NULL pointer exception, effectively crashing the pbx_exchange process. **CVE ID : CVE-2022-42306**	https://www.veritas.com/content/support/en_US/security/VTS22-010#M1	A-VER-NETB-201022/766
Vendor: Vmware					
Product: cloud_foundation					
Affected Version(s): 4.4					
NULL Pointer Dereference	07-Oct-2022	6.5	VMware ESXi contains a null-pointer deference vulnerability. A malicious actor with privileges within the VMX process only, may create a denial of service condition on the host. **CVE ID : CVE-2022-31681**	https://www.vmware.com/security/advisories/VMSA-2022-0025.html	A-VMW-CLOU-201022/767
Affected Version(s): 4.4.1					
NULL Pointer Dereference	07-Oct-2022	6.5	VMware ESXi contains a null-pointer deference vulnerability. A	https://www.vmware.com/security/advisorie	A-VMW-CLOU-201022/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious actor with privileges within the VMX process only, may create a denial of service condition on the host. **CVE ID : CVE-2022-31681**	s/VMSA-2022-0025.html	
Affected Version(s): 4.4.1.1					
NULL Pointer Dereference	07-Oct-2022	6.5	VMware ESXi contains a null-pointer deference vulnerability. A malicious actor with privileges within the VMX process only, may create a denial of service condition on the host. **CVE ID : CVE-2022-31681**	https://www.vmware.com/security/advisories/VMSA-2022-0025.html	A-VMW-CLOU-201022/769
Affected Version(s): From (including) 4.2 Up to (excluding) 4.3.1.1					
NULL Pointer Dereference	07-Oct-2022	6.5	VMware ESXi contains a null-pointer deference vulnerability. A malicious actor with privileges within the VMX process only, may create a denial of service condition on the host. **CVE ID : CVE-2022-31681**	https://www.vmware.com/security/advisories/VMSA-2022-0025.html	A-VMW-CLOU-201022/770
Product: rabbitmq					
Affected Version(s): * Up to (excluding) 3.8.32					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficiently Random Values	06-Oct-2022	7.5	RabbitMQ is a multi-protocol messaging and streaming broker. In affected versions the shovel and federation plugins perform URI obfuscation in their worker (link) state. The encryption key used to encrypt the URI was seeded with a predictable secret. This means that in case of certain exceptions related to Shovel and Federation plugins, reasonably easily deobfuscatable data could appear in the node log. Patched versions correctly use a cluster-wide secret for that purpose. This issue has been addressed and Patched versions: `3.10.2`, `3.9.18`, `3.8.32` are available. Users unable to upgrade should disable the Shovel and Federation plugins. **CVE ID : CVE-2022-31008**	https://github.com/rabbitmq/rabbitmq-server/pull/4841, https://github.com/rabbitmq/rabbitmq-server/security/advisories/GHSA-v9gv-xp36-jgj8	A-VMW-RABB-201022/771
Affected Version(s): From (including) 3.10.0 Up to (excluding) 3.10.2					
Use of Insufficient	06-Oct-2022	7.5	RabbitMQ is a multi-protocol	https://github.com/rabbitmq/	A-VMW-RABB-201022/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			messaging and streaming broker. In affected versions the shovel and federation plugins perform URI obfuscation in their worker (link) state. The encryption key used to encrypt the URI was seeded with a predictable secret. This means that in case of certain exceptions related to Shovel and Federation plugins, reasonably easily deobfuscatable data could appear in the node log. Patched versions correctly use a cluster-wide secret for that purpose. This issue has been addressed and Patched versions: `3.10.2`, `3.9.18`, `3.8.32` are available. Users unable to upgrade should disable the Shovel and Federation plugins. **CVE ID : CVE-2022-31008**	rabbitmq-server/pull/4841, https://github.com/rabbitmq/rabbitmq-server/security/advisories/GHSA-v9gv-xp36-jgj8	
Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.9.18					
Use of Insufficiently Random Values	06-Oct-2022	7.5	RabbitMQ is a multi-protocol messaging and streaming broker.	https://github.com/rabbitmq/rabbitmq-server/pull/48	A-VMW-RABB-201022/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In affected versions the shovel and federation plugins perform URI obfuscation in their worker (link) state. The encryption key used to encrypt the URI was seeded with a predictable secret. This means that in case of certain exceptions related to Shovel and Federation plugins, reasonably easily deobfuscatable data could appear in the node log. Patched versions correctly use a cluster-wide secret for that purpose. This issue has been addressed and Patched versions: `3.10.2`, `3.9.18`, `3.8.32` are available. Users unable to upgrade should disable the Shovel and Federation plugins. **CVE ID : CVE-2022-31008**	41, https://github.com/rabbitmq/rabbitmq-server/security/advisories/GHSA-v9gv-xp36-jgj8	
Product: vcenter_server					
Affected Version(s): * Up to (excluding) 6.5					
Deserialization of Untrusted Data	07-Oct-2022	9.1	The vCenter Server contains an unsafe deserialisation vulnerability in the PSC (Platform	https://www.vmware.com/security/advisorie	A-VMW-VCEN-201022/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			services controller). A malicious actor with admin access on vCenter server may exploit this issue to execute arbitrary code on the underlying operating system that hosts the vCenter Server. **CVE ID : CVE-2022-31680**	s/VMSA-2022-0025.html	
Affected Version(s): 6.5					
Deserialization of Untrusted Data	07-Oct-2022	9.1	The vCenter Server contains an unsafe deserialisation vulnerability in the PSC (Platform services controller). A malicious actor with admin access on vCenter server may exploit this issue to execute arbitrary code on the underlying operating system that hosts the vCenter Server. **CVE ID : CVE-2022-31680**	https://www.vmware.com/security/advisories/VMSA-2022-0025.html	A-VMW-VCEN-201022/775
Product: vrealize_operations					
Affected Version(s): From (including) 8.0 Up to (excluding) 8.10					
N/A	11-Oct-2022	4.9	VMware Aria Operations contains an arbitrary file read vulnerability. A malicious actor with administrative privileges may be	https://www.vmware.com/security/advisories/VMSA-2022-0026.html	A-VMW-VREA-201022/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to read arbitrary files containing sensitive data. **CVE ID : CVE-2022-31682**		
Vendor: web-based_student_clearance_system_project					
Product: web-based_student_clearance_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	09-Oct-2022	7.5	A vulnerability classified as critical was found in SourceCodester Web-Based Student Clearance System 1.0. Affected by this vulnerability is an unknown functionality of the file edit-photo.php of the component Photo Handler. The manipulation leads to unrestricted upload. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-210367. **CVE ID : CVE-2022-3436**	N/A	A-WEB-WEB--201022/777
Improper Neutralization of Input During Web Page Generation	08-Oct-2022	5.4	A vulnerability was found in SourceCodester Web-Based Student Clearance System. It has been rated as problematic. Affected by this issue is the function	N/A	A-WEB-WEB--201022/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			prepare of the file /Admin/add-student.php. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210356. **CVE ID : CVE-2022-3434**		
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	9.8	A vulnerability was found in SourceCodester Web-Based Student Clearance System. It has been classified as critical. Affected is an unknown function of the file /Admin/login.php of the component POST Parameter Handler. The manipulation of the argument txtusername leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-210246 is the	N/A	A-WEB-WEB--201022/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier assigned to this vulnerability. **CVE ID : CVE-2022-3414**		
Vendor: webgilde					
Product: advanced_comment_form					
Affected Version(s): * Up to (excluding) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2022	4.8	The Advanced Comment Form WordPress plugin before 1.2.1 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-3220**	N/A	A-WEB-ADVA-201022/780
Vendor: webpack.js					
Product: loader-utils					
Affected Version(s): 2.0.0					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	12-Oct-2022	9.8	Prototype pollution vulnerability in function parseQuery in parseQuery.js in webpack loader-utils 2.0.0 via the name variable in parseQuery.js. **CVE ID : CVE-2022-37601**	N/A	A-WEB-LOAD-201022/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	11-Oct-2022	7.5	A Regular expression denial of service (ReDoS) flaw was found in Function interpolateName in interpolateName.js in webpack loader-utils 2.0.0 via the resourcePath variable in interpolateName.js. **CVE ID : CVE-2022-37599**	N/A	A-WEB-LOAD-201022/782
Vendor: wedding_planner_project					
Product: wedding_planner					
Affected Version(s): 1.0					
N/A	07-Oct-2022	9.8	Wedding Planner v1.0 is vulnerable to arbitrary code execution. **CVE ID : CVE-2022-42075**	N/A	A-WED-WEDD-201022/783
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	8.8	Wedding Planner v1.0 is vulnerable to arbitrary code execution via users_profile.php. **CVE ID : CVE-2022-42034**	N/A	A-WED-WEDD-201022/784
Unrestricted Upload of File with Dangerous Type	11-Oct-2022	8.8	Wedding Planner v1.0 is vulnerable to Arbitrary code execution via package_edit.php. **CVE ID : CVE-2022-42229**	N/A	A-WED-WEDD-201022/785
Vendor: woo_billingo_plus_project					
Product: woo_billingo_plus					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.4.5.4					
Cross-Site Request Forgery (CSRF)	10-Oct-2022	7.1	The Woo Billingo Plus WordPress plugin before 4.4.5.4, Integration for Billingo & Gravity Forms WordPress plugin before 1.0.4, Integration for Szamlazz.hu & Gravity Forms WordPress plugin before 1.2.7 are lacking CSRF checks in various AJAX actions, which could allow attackers to make logged in Shop Managers and above perform unwanted actions, such as deactivate the plugin's license **CVE ID : CVE-2022-3154**	N/A	A-WOO-WOO_-201022/786
Vendor: wpchill					
Product: download_monitor					
Affected Version(s): * Up to (excluding) 4.5.98					
Files or Directories Accessible to External Parties	10-Oct-2022	4.9	The Download Monitor WordPress plugin before 4.5.98 does not ensure that files to be downloaded are inside the blog folders, and not sensitive, allowing high privilege users such as admin to download the wp-	N/A	A-WPC-DOWN-201022/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			config.php or /etc/passwd even in an hardened environment or multisite setup. **CVE ID : CVE-2022-2981**		
Vendor: wpdarko					
Product: top_bar					
Affected Version(s): * Up to (excluding) 3.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Oct-2022	4.8	The Top Bar WordPress plugin before 3.0.4 does not sanitise and escape some of its settings before outputting them in frontend pages, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2629**	N/A	A-WPD-TOP_-201022/788
Vendor: wpsocialrocket					
Product: social_rocket					
Affected Version(s): * Up to (excluding) 1.3.3					
Improper Neutralization of Input During Web Page Generation	10-Oct-2022	4.8	The Social Rocket WordPress plugin before 1.3.3 does not sanitise and escape some of its settings, which could allow high	N/A	A-WPS-SOCI-201022/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-3136**		
Vendor: wpwhitesecurity					
Product: wp_2fa					
Affected Version(s): * Up to (excluding) 2.3.0					
Exposure of Sensitive Information to an Unauthorized Actor	10-Oct-2022	5.9	The WP 2FA WordPress plugin before 2.3.0 uses comparison operators that don't mitigate time-based attacks, which could be abused to leak information about the authentication codes being compared. **CVE ID : CVE-2022-2891**	N/A	A-WPW-WP_2-201022/790
Vendor: wp_socializer_project					
Product: wp_socializer					
Affected Version(s): * Up to (excluding) 7.3					
Improper Neutralization of Input During Web Page Generation	03-Oct-2022	4.8	The WP Socializer WordPress plugin before 7.3 does not sanitise and escape some of its Icons settings, which could allow high privilege users such	N/A	A-WP_-WP_S-201022/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2763**		
Vendor: xgenecloud					
Product: nocodb					
Affected Version(s): * Up to (excluding) 0.92.0					
Uncontrolled Resource Consumption	07-Oct-2022	6.5	Denial of Service in GitHub repository nocodb/nocodb prior to 0.92.0. **CVE ID : CVE-2022-3423**	https://huntr.dev/bounties/94639d8e-8301-4432-ab80-e76e1346e631, https://github.com/nocodb/nocodb/commit/000ecd886738b965b5997cd905825e3244f48b95	A-XGE-NOCO-201022/792
Vendor: xmldom_project					
Product: xmldom					
Affected Version(s): From (including) 0.6.0 Up to (excluding) 0.8.3					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	11-Oct-2022	9.8	A prototype pollution vulnerability exists in the function copy in dom.js in the xmldom (published as @xmldom/xmldom) package before 0.8.3 for Node.js via the p variable.	https://github.com/xmldom/xmldom/blob/bc36efddf9948aba15618f85dc1addfc2ac9d7b2/lib/dom.js#L1, https://github.com/xmldom/xmldom/issues/436, https://github.	A-XML-XMLD-201022/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37616	com/xmldom/xmldom/blob/bc36efddf9948aba15618f85dc1addfc2ac9d7b2/lib/dom.js#L3, https://github.com/xmldom/xmldom/blob/bc36efddf9948aba15618f85dc1addfc2ac9d7b2/lib/dom.js#L1	
Vendor: yetiforce					
Product: yetiforce_customer_relationship_management					
Affected Version(s): * Up to (excluding) 6.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0. **CVE ID : CVE-2022-3002**	https://github.com/yetiforcecompany/yetiforcecrm/commit/54728becfdad9b6e686bbe336007cba2ce518248, https://huntr.dev/bounties/d213d7ea-fe92-40b2-a1f9-2ba32dec50f5	A-YET-YETI-201022/794
Vendor: zephyr-one					
Product: zephyr_project_manager					
Affected Version(s): * Up to (excluding) 3.2.55					
Cross-Site Request Forgery (CSRF)	03-Oct-2022	5.4	The Zephyr Project Manager WordPress plugin before 3.2.55 does not have any authorisation as well as CSRF in all its AJAX actions, allowing	N/A	A-ZEP-ZEPH-201022/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated users to call them either directly or via CSRF attacks. Furthermore, due to the lack of sanitisation and escaping, it could also allow them to perform Stored Cross-Site Scripting attacks against logged in admins. **CVE ID : CVE-2022-2839**		
Vendor: Zimbra					
Product: collaboration					
Affected Version(s): 8.8.15					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Oct-2022	6.1	In Zimbra Collaboration Suite (ZCS) 8.8.15, the URL at /h/compose accepts an attachUrl parameter that is vulnerable to Reflected XSS. This allows executing arbitrary JavaScript on the victim's machine. **CVE ID : CVE-2022-41349**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-201022/796
Improper Neutralization of Input During Web Page Generation	12-Oct-2022	6.1	In Zimbra Collaboration Suite (ZCS) 8.8.15, /h/search?action=voicemail&action=listen accepts a phone parameter that is vulnerable to Reflected XSS. This	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-201022/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			allows executing arbitrary JavaScript on the victim's machine. **CVE ID : CVE-2022-41350**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Oct-2022	6.1	In Zimbra Collaboration Suite (ZCS) 8.8.15, at the URL /h/calendar, one can trigger XSS by adding JavaScript code to the view parameter and changing the value of the uncheck parameter to a string (instead of default value of 10). **CVE ID : CVE-2022-41351**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-201022/798
Affected Version(s): 9.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Oct-2022	6.1	An issue was discovered in Zimbra Collaboration (ZCS) 9.0. XSS can occur via the onerror attribute of an IMG element, leading to information disclosure. **CVE ID : CVE-2022-41348**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-201022/799
Vendor: zinclabs					
Product: zinc					
Affected Version(s): From (including) 0.1.9 Up to (including) 0.3.1					
Improper Neutralization of	06-Oct-2022	5.4	In Zinc, versions v0.1.9 through v0.3.1 are	https://github.com/zinclabs/zinc/commit/33	A-ZIN-ZINC-201022/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerable to Stored Cross-Site Scripting when using the delete user functionality. When an authenticated user deletes a user having a XSS payload in the user id field, the javascript payload will be executed and allow an attacker to access the user's credentials. **CVE ID : CVE-2022-32171**	76c248bade163430f9347742428f0a82cd322d	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-2022	5.4	In Zinc, versions v0.1.9 through v0.3.1 are vulnerable to Stored Cross-Site Scripting when using the delete template functionality. When an authenticated user deletes a template with a XSS payload in the name field, the Javascript payload will be executed and allow an attacker to access the user's credentials. **CVE ID : CVE-2022-32172**	https://github.com/zinclabs/zinc/commit/3376c248bade163430f9347742428f0a82cd322d	A-ZIN-ZINC-201022/801
Vendor: zkteco					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: zkbiosecurity_v5000					
Affected Version(s): 3.0.5.0_r					
Incorrect Authorization	07-Oct-2022	8.8	An access control issue in ZKTeco ZKBioSecurity V5000 3.0.5_r allows attackers to arbitrarily create admin users via a crafted HTTP request. **CVE ID : CVE-2022-36634**	N/A	A-ZKT-ZKBI-201022/802
Affected Version(s): 4.1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-2022	8.8	ZKteco ZKBioSecurity V5000 4.1.3 was discovered to contain a SQL injection vulnerability via the component /baseOpLog.do. **CVE ID : CVE-2022-36635**	N/A	A-ZKT-ZKBI-201022/803
Vendor: Zoneminder					
Product: Zoneminder					
Affected Version(s): * Up to (excluding) 1.36.27					
Improper Authentication	07-Oct-2022	6.5	ZoneMinder is a free, open source Closed-circuit television software application. In affected versions authenticated users can bypass CSRF keys by modifying the request supplied to the Zoneminder web application. These	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-xgv6-qv6c-399q, https://github.com/ZoneMinder/zoneminder/commit/c0a4c05e84eea0f6ccf	A-ZON-ZONE-201022/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifications include replacing HTTP POST with an HTTP GET and removing the CSRF key from the request. An attacker can take advantage of this by using an HTTP GET request to perform actions with no CSRF protection. This could allow an attacker to cause an authenticated user to perform unexpected actions on the web application. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue. **CVE ID : CVE-2022-39290**	7169c014efe5422c9ba0d	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	5.4	ZoneMinder is a free, open source Closed-circuit television software application The file parameter is vulnerable to a cross site scripting vulnerability (XSS) by backing out of the current "tr" "td" brackets. This then allows a malicious user to provide code that will	https://github.com/ZoneMinder/zoneminder/commit/c0a4c05e84eea0f6ccf7169c014efe5422c9ba0d, https://github.com/ZoneMinder/zoneminder/commit/d289eb48601a76e34feea3c1683955337b1fae59	A-ZON-ZONE-201022/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute when a user views the specific log on the "view=log" page. This vulnerability allows an attacker to store code within the logs that will be executed when loaded by a legitimate user. These actions will be performed with the permission of the victim. This could lead to data loss and/or further exploitation including account takeover. This issue has been addressed in versions `1.36.27` and `1.37.24`. Users are advised to upgrade. Users unable to upgrade should disable database logging. **CVE ID : CVE-2022-39285**		
Improper Input Validation	07-Oct-2022	5.4	ZoneMinder is a free, open source Closed-circuit television software application. Affected versions of zoneminder are subject to a vulnerability which allows users with "View" system permissions to	https://github.com/ZoneMinder/zoneminder/commit/34ffd92bf123070cab6c83ad4cfe6297dd0ed0b4, https://github.com/ZoneMinder/zoneminder/commit/cb3fc5907da21a511	A-ZON-ZONE-201022/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject new data into the logs stored by Zoneminder. This was observed through an HTTP POST request containing log information to the "/zm/index.php" endpoint. Submission is not rate controlled and could affect database performance and/or consume all storage resources. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-39291**	1ae54128a5d0b49ae755e9b	
Affected Version(s): * Up to (including) 1.36.27					
Improper Authentication	07-Oct-2022	7.5	ZoneMinder is a free, open source Closed-circuit television software application. In affected versions the ZoneMinder API Exposes Database Log contents to user without privileges, allows insertion, modification, deletion of logs without System Privileges. Users are advised yo upgrade as soon as	https://github.com/ZoneMinder/zoneminder/commit/34ffd92bf123070cab6c83ad4cfe6297dd0ed0b4, https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-mpcx-3gvh-9488	A-ZON-ZONE-201022/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible. Users unable to upgrade should disable database logging. **CVE ID : CVE-2022-39289**		
Affected Version(s): From (excluding) 1.37.0 Up to (excluding) 1.37.24					
Improper Authentication	07-Oct-2022	6.5	ZoneMinder is a free, open source Closed-circuit television software application. In affected versions authenticated users can bypass CSRF keys by modifying the request supplied to the Zoneminder web application. These modifications include replacing HTTP POST with an HTTP GET and removing the CSRF key from the request. An attacker can take advantage of this by using an HTTP GET request to perform actions with no CSRF protection. This could allow an attacker to cause an authenticated user to perform unexpected actions on the web application. Users are advised to upgrade as soon as possible. There are	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-xgv6-qv6c-399q, https://github.com/ZoneMinder/zoneminder/commit/c0a4c05e84eea0f6ccf7169c014efe5422c9ba0d	A-ZON-ZONE-201022/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no known workarounds for this issue. **CVE ID : CVE-2022-39290**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	5.4	ZoneMinder is a free, open source Closed-circuit television software application The file parameter is vulnerable to a cross site scripting vulnerability (XSS) by backing out of the current "tr" "td" brackets. This then allows a malicious user to provide code that will execute when a user views the specific log on the "view=log" page. This vulnerability allows an attacker to store code within the logs that will be executed when loaded by a legitimate user. These actions will be performed with the permission of the victim. This could lead to data loss and/or further exploitation including account takeover. This issue has been addressed in versions `1.36.27` and	https://github.com/ZoneMinder/zoneminder/commit/c0a4c05e84eea0f6ccf7169c014efe5422c9ba0d, https://github.com/ZoneMinder/zoneminder/commit/d289eb48601a76e34feea3c1683955337b1fae59	A-ZON-ZONE-201022/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`1.37.24`. Users are advised to upgrade. Users unable to upgrade should disable database logging. **CVE ID : CVE-2022-39285**		
Improper Input Validation	07-Oct-2022	5.4	ZoneMinder is a free, open source Closed-circuit television software application. Affected versions of zoneminder are subject to a vulnerability which allows users with "View" system permissions to inject new data into the logs stored by Zoneminder. This was observed through an HTTP POST request containing log information to the "/zm/index.php" endpoint. Submission is not rate controlled and could affect database performance and/or consume all storage resources. Users are advised to upgrade. There are no known workarounds for this issue.	https://github.com/ZoneMinder/zoneminder/commit/34ffd92bf123070cab6c83ad4cfe6297dd0ed0b4, https://github.com/ZoneMinder/zoneminder/commit/cb3fc5907da21a5111ae54128a5d0b49ae755e9b	A-ZON-ZONE-201022/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39291		
Affected Version(s): From (including) 1.37.0 Up to (excluding) 1.37.24					
Improper Authentication	07-Oct-2022	7.5	ZoneMinder is a free, open source Closed-circuit television software application. In affected versions the ZoneMinder API Exposes Database Log contents to user without privileges, allows insertion, modification, deletion of logs without System Privileges. Users are advised yo upgrade as soon as possible. Users unable to upgrade should disable database logging. **CVE ID : CVE-2022-39289**	https://github.com/ZoneMinder/zoneminder/commit/34ffd92bf123070cab6c83ad4cfe6297dd0ed0b4, https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-mpcx-3gvh-9488	A-ZON-ZONE-201022/811
Hardware					
Vendor: arraynetworks					
Product: ag1000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE:	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Re	H-ARR-AG10-201022/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	mote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	
Product: ag1000t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-AG10-201022/813
Product: ag1000v5					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-AG10-201022/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ag1100v5					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-AG11-201022/815
Product: ag1150					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-AG11-201022/816
Product: ag1200					
Affected Version(s): -					
Improper Neutralization of	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before	https://support.arraynetworks.net/prx/001/h	H-ARR-AG12-201022/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	ttp/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	
Product: ag1200v5					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-AG12-201022/818
Product: ag1500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Securit	H-ARR-AG15-201022/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	y_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	
Product: ag1500fips					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-AG15-201022/820
Product: ag1500v5					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-	H-ARR-AG15-201022/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				11961_%20V2.1.pdf	
Product: ag1600					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-AG16-201022/822
Product: ag1600v5					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-AG16-201022/823
Product: ah1100					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-AH11-201022/824
Product: vxag					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	H-ARR-VXAG-201022/825
Vendor: Arubanetworks					
Product: ap-103					
Affected Version(s): -					
Buffer Copy without Checking Size of	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could	https://www.arubanetworks.com/assets/aler	H-ARU-AP-1-201022/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities.	t/ARUBA-PSA-2022-014.txt	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37888		
Product: ap-114					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-1-201022/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-115					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-1-201022/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-120					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-1-201022/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-121					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-1-201022/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-130					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-1-201022/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-135					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-1-201022/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-204					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-2-201022/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-205					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-2-201022/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-207					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-2-201022/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-214					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-2-201022/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-215					
Affected Version(s): -					
Buffer Copy without	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in	https://www.arubanetworks.com/assets/aler	H-ARU-AP-2-201022/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities.	t/ARUBA-PSA-2022-014.txt	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37888		
Product: ap-224					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-2-201022/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-225					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-2-201022/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-303					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-304					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-305					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-314					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-315					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-318					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-324					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-325					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-334					
Affected Version(s): -					
Buffer Copy without	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in	https://www.arubanetworks.com/assets/aler	H-ARU-AP-3-201022/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities.	t/ARUBA-PSA-2022-014.txt	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37888		
Product: ap-340					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-370					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-3-201022/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-504					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-5-201022/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-505					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-5-201022/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-514					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-5-201022/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-515					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-5-201022/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-534					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-5-201022/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-535					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-5-201022/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-555					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-5-201022/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-635					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-AP-6-201022/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: ap-655					
Affected Version(s): -					
Buffer Copy without	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in	https://www.arubanetworks.com/assets/aler	H-ARU-AP-6-201022/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities.	t/ARUBA-PSA-2022-014.txt	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37888		
Product: iap-103					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-114					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-115					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-204					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-205					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-207					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-224					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-225					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-304					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-305					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-314					
Affected Version(s): -					
Buffer Copy without	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in	https://www.arubanetworks.com/assets/aler	H-ARU-IAP--201022/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities.	t/ARUBA-PSA-2022-014.txt	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37888		
Product: iap-315					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-318					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-324					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-325					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: iap-334					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-IAP--201022/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: rap-108					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-RAP--201022/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Product: rap-109					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	H-ARU-RAP--201022/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Vendor: bushnellgolf					
Product: launch_pro					
Affected Version(s): -					
Incorrect Default Permissions	13-Oct-2022	8	Foresight GC3 Launch Monitor 1.3.15.68 ships with a Target Communication Framework (TCF) service enabled. This service listens on a TCP port on all interfaces and allows for process debugging, file system modification, and terminal access as the root user. In conjunction with a hosted wireless access point and the known passphrase of FSSPORTS, an attacker could use this service to modify a device and	N/A	H-BUS-LAUN-201022/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			steal intellectual property. **CVE ID : CVE-2022-40187**		
Vendor: Cisco					
Product: asr_1000-esp100-x					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	10-Oct-2022	8.6	A vulnerability in the DNS application layer gateway (ALG) functionality that is used by Network Address Translation (NAT) in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. This vulnerability is due to a logic error that occurs when an affected device inspects certain TCP DNS packets. An attacker could exploit this vulnerability by sending crafted DNS packets through the affected device that is performing NAT for DNS packets. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-alg-dos-KU9Z8kFX	H-CIS-ASR_-201022/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition on the affected device. Note: This vulnerability can be exploited only by sending IPv4 TCP packets through an affected device. This vulnerability cannot be exploited by sending IPv6 traffic. **CVE ID : CVE-2022-20837**		
Product: asr_1000-esp200-x					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	10-Oct-2022	8.6	A vulnerability in the DNS application layer gateway (ALG) functionality that is used by Network Address Translation (NAT) in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. This vulnerability is due to a logic error that occurs when an affected device inspects certain TCP DNS packets. An attacker could exploit this vulnerability by sending crafted DNS packets through the affected device that	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-alg-dos-KU9Z8kFX	H-CIS-ASR_-201022/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is performing NAT for DNS packets. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition on the affected device. Note: This vulnerability can be exploited only by sending IPv4 TCP packets through an affected device. This vulnerability cannot be exploited by sending IPv6 traffic. **CVE ID : CVE-2022-20837**		
Product: catalyst_3650					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-12x48fd-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3650-12x48fd-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/886
Product: catalyst_3650-12x48fd-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-12x48uq					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-12x48uq-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-12x48uq-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/894
Product: catalyst_3650-12x48uq-s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/895
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3650-12x48ur					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-12x48ur-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-12x48ur-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3650-12x48ur-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/904
Product: catalyst_3650-12x48uz					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-12x48uz-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-12x48uz-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-12x48uz-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/912
Product: catalyst_3650-24pd					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/913
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3650-24pd-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-24pd-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-24pd-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3650-24pdm					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/922
Product: catalyst_3650-24pdm-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-24pdm-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-24pdm-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-24ps-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/930
Product: catalyst_3650-24ps-l					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/931
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3650-24ps-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-24td-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-24td-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3650-24td-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/940
Product: catalyst_3650-24ts-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-24ts-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-24ts-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48fd-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/948
Product: catalyst_3650-48fd-l					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/949
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3650-48fd-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48fq					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48fq-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3650-48fq-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/958
Product: catalyst_3650-48fq-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48fqm					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48fqm-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48fqm-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/966
Product: catalyst_3650-48fqm-s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/967
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3650-48fs-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48fs-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48fs-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3650-48pd-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/976
Product: catalyst_3650-48pd-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48pd-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48pq-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48pq-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/984
Product: catalyst_3650-48pq-s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/985
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3650-48ps-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48ps-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48ps-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3650-48td-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/994
Product: catalyst_3650-48td-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48td-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48tq-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48tq-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1002
Product: catalyst_3650-48tq-s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1003
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3650-48ts-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48ts-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-48ts-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3650-8x24pd-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1012
Product: catalyst_3650-8x24pd-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-8x24pd-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-8x24uq					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3650-8x24uq-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1020
Product: catalyst_3650-8x24uq-l					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1021
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3650-8x24uq-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-12s-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3850-12s-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1030
Product: catalyst_3850-12x48u					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-12xs-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-12xs-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-16xs-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1038
Product: catalyst_3850-16xs-s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1039
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3850-24p-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24p-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24p-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3850-24pw-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1048
Product: catalyst_3850-24s-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24s-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24t-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24t-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1056
Product: catalyst_3850-24t-s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1057
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3850-24u					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24u-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24u-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3850-24u-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1066
Product: catalyst_3850-24xs					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24xs-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24xs-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24xu					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1074
Product: catalyst_3850-24xu-e					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1075
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3850-24xu-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-24xu-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-32xs-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3850-32xs-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1084
Product: catalyst_3850-48f-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48f-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48f-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48p-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1092
Product: catalyst_3850-48p-l					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1093
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3850-48p-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48pw-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48t-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3850-48t-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1102
Product: catalyst_3850-48t-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48u					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48u-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48u-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1110
Product: catalyst_3850-48u-s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1111
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_3850-48xs					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48xs-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-48xs-f-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_3850-48xs-f-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1120
Product: catalyst_3850-48xs-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-nm-2-40g					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_3850-nm-8-10g					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_8500					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	10-Oct-2022	8.6	A vulnerability in the DNS application layer gateway (ALG) functionality that is used by Network Address Translation (NAT) in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. This vulnerability is due to a logic error that occurs when an affected device inspects certain TCP DNS packets. An attacker could exploit this vulnerability by sending crafted DNS packets through the affected device that is performing NAT for DNS packets. A successful exploit could allow the attacker to cause the device to reload, resulting in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-alg-dos-KU9Z8kFX	H-CIS-CATA-201022/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition on the affected device. Note: This vulnerability can be exploited only by sending IPv4 TCP packets through an affected device. This vulnerability cannot be exploited by sending IPv6 traffic. **CVE ID : CVE-2022-20837**		
Product: catalyst_8500-4qc					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	10-Oct-2022	8.6	A vulnerability in the DNS application layer gateway (ALG) functionality that is used by Network Address Translation (NAT) in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. This vulnerability is due to a logic error that occurs when an affected device inspects certain TCP DNS packets. An attacker could exploit this vulnerability by sending crafted DNS packets through the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-alg-dos-KU9Z8kFX	H-CIS-CATA-201022/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device that is performing NAT for DNS packets. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition on the affected device. Note: This vulnerability can be exploited only by sending IPv4 TCP packets through an affected device. This vulnerability cannot be exploited by sending IPv6 traffic. **CVE ID : CVE-2022-20837**		
Product: catalyst_9200					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_9200cx					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9200l					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20870		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1136
Product: catalyst_9300-24p-a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1137
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_9300-24p-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-24s-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-24s-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_9300-24t-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1146
Product: catalyst_9300-24t-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-24u-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-24u-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-24ux-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1154
Product: catalyst_9300-24ux-e					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1155
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_9300-48p-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-48p-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-48s-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_9300-48s-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1164
Product: catalyst_9300-48t-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-48t-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-48u-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-48u-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1172
Product: catalyst_9300-48un-a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1173
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_9300-48un-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-48uxm-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300-48uxm-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_9300l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1182
Product: catalyst_9300l-24p-4g-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300l-24p-4g-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300l-24p-4x-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300l-24p-4x-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1190
Product: catalyst_9300l-24t-4g-a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1191
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_9300l-24t-4g-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300l-24t-4x-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300l-24t-4x-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_9300l-48p-4g-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1200
Product: catalyst_9300l-48p-4g-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300l-48p-4x-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300l-48p-4x-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300l-48t-4g-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1208
Product: catalyst_9300l-48t-4g-e					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1209
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_9300l-48t-4x-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300l-48t-4x-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9300lm					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_9300l_stack					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1217
Product: catalyst_9300x					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1218
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_9400					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9407r					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9410r					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9500					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_9500h					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20870		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1227
Product: catalyst_9600					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1228
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_9600x					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c2928-24lt-c					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c2928-48tc-c					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c3850-12x48u-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c3850-12x48u-l					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: catalyst_c3850-12x48u-s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1237
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	yAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_c9200-24p					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-	H-CIS-CATA-201022/1239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE	verify-D4NEQA6q	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200-24t					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-	https://tools.cisco.com/securit	H-CIS-CATA-201022/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	y/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_c9200-48p					
Affected Version(s): -					
Improper Verification of Cryptograp	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-	H-CIS-CATA-201022/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on	verify-D4NEQA6q	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200-48t					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1246
Product: catalyst_c9200l-24p-4g					
Affected Version(s): -					
Improper Verification of Cryptograp	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or	yAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200l-24p-4x					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20944		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1250
Product: catalyst_c9200l-24pxg-2y					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200l-24pxg-4x					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: catalyst_c9200l-24t-4g					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200l-24t-4x					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_c9200l-48p-4g					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200l-48p-4x					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200l-48pxg-2y					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200l-48pxg-4x					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200l-48t-4g					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9200l-48t-4x					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	H-CIS-CATA-201022/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9300-24p					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9300-24s					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_c9300-24t					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1273
Product: catalyst_c9300-24u					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1274
Product: catalyst_c9300-24ux					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-	https://tools.cisco.com/securit	H-CIS-CATA-201022/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	y/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_c9300-48p					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_c9300-48s					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9300-48t					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9300-48u					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9300-48un					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9300-48uxm					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9300l-24p-4g					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9300l-24p-4x					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9300l-24t-4g					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_c9300l-24t-4x					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1285
Product: catalyst_c9300l-48p-4g					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1286
Product: catalyst_c9300l-48p-4x					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-	https://tools.cisco.com/securit	H-CIS-CATA-201022/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	y/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_c9300l-48t-4g					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_c9300l-48t-4x					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9404r					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9407r					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9410r					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9500-12q					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9500-12q-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20870		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1296
Product: catalyst_c9500-12q-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1297
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_c9500-16x					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9500-16x-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9500-16x-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_c9500-24q					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1306
Product: catalyst_c9500-24q-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9500-24q-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9500-24y4c					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9500-32c					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1314
Product: catalyst_c9500-32qc					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1315
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-CATA-201022/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	o-sa-iosxe-info-disc-nrORXjO	
Product: catalyst_c9500-40x					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9500-40x-a					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9500-40x-e					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20864		
Product: catalyst_c9500-48y4c					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1324
Product: catalyst_c9600-lc-24c					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-CATA-201022/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	yAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9600-lc-48s					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9600-lc-48tx					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Product: catalyst_c9600-lc-48yl					
Affected Version(s): -					
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	H-CIS-CATA-201022/1331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**		
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	H-CIS-CATA-201022/1332
Vendor: Dell					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: alienware_area-51_r4					
Affected Version(s): -					
Use of Uninitialized Resource	12-Oct-2022	7.8	Dell BIOS contains a use of uninitialized variable vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-34390**	https://www.dell.com/support/kbdoc/000203882	H-DEL-ALIE-201022/1333
N/A	12-Oct-2022	7.8	Dell Client BIOS Versions prior to the remediated version contain an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-34391**	https://www.dell.com/support/kbdoc/000203882	H-DEL-ALIE-201022/1334
Product: alienware_area-51_r5					
Affected Version(s): -					
Use of Uninitialized Resource	12-Oct-2022	7.8	Dell BIOS contains a use of uninitialized variable vulnerability. A local authenticated malicious user may	https://www.dell.com/support/kbdoc/000203882	H-DEL-ALIE-201022/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-34390**		
N/A	12-Oct-2022	7.8	Dell Client BIOS Versions prior to the remediated version contain an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-34391**	https://www.dell.com/support/kbdoc/000203882	H-DEL-ALIE-201022/1336
Product: alienware_area_51m_r1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1338
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1339
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1341
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1342
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1344
Product: alienware_area_51m_r2					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1345
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1347
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1348
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1350
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1351
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: alienware_aurora_r10					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1353
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1354
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1356
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1357
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1359
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1360
Product: alienware_aurora_r11					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1362
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1363
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1365
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1366
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1368
Product: alienware_aurora_r12					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1369
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1371
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1372
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1374
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1375
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: alienware_aurora_r13					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1377
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1379
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1380
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1382
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1383
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: alienware_aurora_r8					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1385
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1386
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1389
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1391
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1392
Product: alienware_aurora_r9					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1394
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1395
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1397
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1398
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1400
Product: alienware_m15_r1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1401
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1403
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1404
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1406
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1407
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: alienware_m15_r2					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1409
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1410
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1412
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1413
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1415
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1416
Product: alienware_m15_r3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1417
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1418
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1420
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1421
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1423
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1424
Product: alienware_m15_r4					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1426
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1427
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1429
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1430
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1432
Product: alienware_m17_r1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1433
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1435
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1436
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1438
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1439
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: alienware_m17_r2					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1441
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1442
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1444
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1445
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1447
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1448
Product: alienware_m17_r3					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1450
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1451
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1453
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1454
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1456
Product: alienware_m17_r4					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1458
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1459
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1461
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1462
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1464
Product: alienware_x14					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1465
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1467
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1468
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1470
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1471
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: alienware_x15_r1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1473
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1474
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1476
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1477
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1479
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1480
Product: alienware_x15_r2					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1482
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1483
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1485
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1486
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1488
Product: alienware_x17_r1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1489
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1491
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1492
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1494
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1495
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: alienware_x17_r2					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1497
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1499
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1500
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1502
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1503
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-ALIE-201022/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: chengming_3980					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1505
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1506
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1508
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1509
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1511
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1512
Product: chengming_3988					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1514
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1515
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1517
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1518
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1520
Product: chengming_3990					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1521
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1523
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1524
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1526
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1527
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: chengming_3991					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1529
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1530
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1532
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1533
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1535
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-CHEN-201022/1536
Product: edge_gateway_3000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1537
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1538
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1540
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1541
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1543
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1544
Product: edge_gateway_5000					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1546
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1547
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1549
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1550
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EDGE-201022/1552
Product: embedded_box_pc_3000					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1553
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1555
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1556
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1558
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1559
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: embedded_box_pc_5000					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1561
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1562
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1564
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1565
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1567
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-EMBE-201022/1568
Product: g3_15_3590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1570
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1571
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1573
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1574
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1576
Product: g3_15_5590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1578
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1579
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1581
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1582
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_1-201022/1584
Product: g3_3579					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1585
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1587
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1588
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1590
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1591
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: g3_3779					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1593
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1594
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1596
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1597
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1599
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G3_3-201022/1600
Product: g5_5000					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1602
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1603
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1605
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1606
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1608
Product: g5_5090					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1609
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1611
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1612
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1614
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1615
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-G5_5-201022/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: g7_17_7590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1617
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1619
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1620
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1622
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1623
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: g7_17_7790					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1625
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1626
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1628
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1629
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1631
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-G7_1-201022/1632
Product: inspiron_14_3467					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1634
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1635
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1637
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1638
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1640
Product: inspiron_15_2-in-1_5582					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1641
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1643
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1644
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1646
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1647
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_15_3567					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1649
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1650
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1652
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1653
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1655
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1656
Product: inspiron_3277					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1657
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1658
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1660
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1661
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1663
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1664
Product: inspiron_3280					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1666
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1667
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1669
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1670
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1672
Product: inspiron_3470					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1673
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1675
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1676
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1678
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1679
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3471					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1681
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1682
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1684
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1685
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1687
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1688
Product: inspiron_3477					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1690
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1691
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1693
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1694
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1696
Product: inspiron_3480					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1698
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1699
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1701
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1702
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1704
Product: inspiron_3481					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1705
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1707
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1708
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1710
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1711
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_3482					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1713
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1714
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1717
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1719
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1720
Product: inspiron_3490					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1722
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1723
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1725
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1726
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1728
Product: inspiron_3493					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1729
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1731
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1732
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1734
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1735
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3501					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1737
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1739
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1740
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1742
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1743
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: inspiron_3502					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1745
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1746
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1748
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1749
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1751
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1752
Product: inspiron_3580					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1754
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1755
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1757
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1758
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1760
Product: inspiron_3581					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1761
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1763
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1764
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1766
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1767
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3582					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1769
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1770
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1772
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1773
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1775
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1776
Product: inspiron_3590					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1777
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1778
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1780
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1781
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1783
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1784
Product: inspiron_3593					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1786
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1787
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1789
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1790
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1792
Product: inspiron_3670					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1793
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1795
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1796
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1798
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1799
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3671					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1801
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1802
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1804
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1805
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1807
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1808
Product: inspiron_3780					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1810
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1811
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1813
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1814
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1816
Product: inspiron_3781					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1818
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1819
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1821
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1822
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1824
Product: inspiron_3782					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1825
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1827
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1828
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1830
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1831
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_3790					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1833
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1834
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1836
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1837
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1839
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1840
Product: inspiron_3793					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1842
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1843
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1845
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1846
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1848
Product: inspiron_3880					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1849
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1851
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1852
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1854
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1855
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3881					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1857
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1859
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1860
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1862
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1863
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: inspiron_5390					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1865
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1866
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1868
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1869
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1871
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1872
Product: inspiron_5391					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1874
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1875
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1877
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1878
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1880
Product: inspiron_5400					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1881
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1883
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1884
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1886
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1887
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5401					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1889
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1890
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1893
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1895
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1896
Product: inspiron_5477					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1897
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1898
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1900
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1901
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1903
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1904
Product: inspiron_5480					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1906
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1907
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1909
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1910
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1912
Product: inspiron_5481					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1913
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1915
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1916
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1918
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1919
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5482					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1921
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1922
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1924
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1925
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1927
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1928
Product: inspiron_5490					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1930
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1931
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1933
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1934
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1936
Product: inspiron_5491_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1938
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1939
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1941
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1942
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1944
Product: inspiron_5491_aio					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1945
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1947
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1948
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1950
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1951
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_5493					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1953
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1954
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1956
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1957
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1959
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1960
Product: inspiron_5494					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1962
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1963
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1965
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1966
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1968
Product: inspiron_5498					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1969
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1971
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1972
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1974
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1975
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5570					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1977
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1979
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1980
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1982
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1983
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: inspiron_5580					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1985
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1986
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1988
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1989
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1991
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1992
Product: inspiron_5583					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1994
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1995
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1997
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1998
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/1999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2000
Product: inspiron_5584					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2001
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2003
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2004
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2006
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2007
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2009
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2010
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2012
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2013
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2015
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2016
Product: inspiron_5591_2-in-1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2017
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2018
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2020
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2021
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2023
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2024
Product: inspiron_5593					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2026
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2027
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2029
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2030
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2032
Product: inspiron_5594					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2033
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2035
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2036
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2038
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2039
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5598					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2041
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2042
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2044
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2045
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2047
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2048
Product: inspiron_5680					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2050
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2051
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2053
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2054
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2056
Product: inspiron_5770					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2058
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2059
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2061
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2062
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2064
Product: inspiron_7000					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2065
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2067
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2068
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2070
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2071
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_7370					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2073
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2074
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2076
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2077
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2079
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2080
Product: inspiron_7373					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2082
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2083
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2085
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2086
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2088
Product: inspiron_7380					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2089
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2091
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2092
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2094
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2095
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_7386					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2097
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2099
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2100
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2102
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2103
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: inspiron_7390					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2105
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2106
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2108
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2109
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2111
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2112
Product: inspiron_7391					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2114
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2115
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2117
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2118
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2120
Product: inspiron_7490					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2121
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2123
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2124
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2126
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2127
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_7570					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2129
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2130
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2132
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2133
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2135
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2136
Product: inspiron_7573					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2137
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2138
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2140
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2141
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2143
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2144
Product: inspiron_7580					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2146
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2147
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2149
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2150
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2152
Product: inspiron_7586					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2153
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2155
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2156
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2158
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2159
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_7590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2161
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2162
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2165
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2167
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2168
Product: inspiron_7591					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2170
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2171
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2173
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2174
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2176
Product: inspiron_7700_aio					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2178
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2179
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2181
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2182
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2184
Product: inspiron_7777					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2185
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2187
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2188
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2190
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2191
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_7786					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2193
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2194
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2196
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2197
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2199
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2200
Product: inspiron_7790					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2202
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2203
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2205
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2206
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2208
Product: inspiron_7791					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2209
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2211
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2212
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2214
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2215
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-INSP-201022/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_3120					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2217
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2219
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2220
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2222
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2223
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_3180					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2225
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2226
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2228
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2229
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2231
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2232
Product: latitude_3189					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2234
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2235
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2237
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2238
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2240
Product: latitude_3190					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2241
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2243
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2244
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2246
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2247
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_3190_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2249
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2250
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2252
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2253
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2255
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2256
Product: latitude_3300					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2257
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2258
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2260
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2261
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2263
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2264
Product: latitude_3301					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2266
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2267
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2269
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2270
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2272
Product: latitude_3310					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2273
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2275
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2276
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2278
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2279
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_3310_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2281
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2282
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2284
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2285
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2287
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2288
Product: latitude_3379					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2290
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2291
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2293
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2294
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2296
Product: latitude_3390					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2298
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2299
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2301
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2302
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2304
Product: latitude_3420					
Affected Version(s): -					
Incorrect Comparison	10-Oct-2022	4.9	Dell Wyse ThinOS 2205 contains a Regular Expression Denial of Service Vulnerability in UI. An admin privilege attacker could potentially exploit this vulnerability, leading to denial-of-service. **CVE ID : CVE-2022-34402**	https://www.dell.com/support/kbdoc/en-us/000203376/dsa-2022-247-dell-wyse-thinos-security-update-for-a-regular-expression-vulnerability	H-DEL-LATI-201022/2305
Product: latitude_3480					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2307
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2308
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2310
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2311
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2313
Product: latitude_3490					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2314
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2316
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2317
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2319
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2320
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_3580					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2322
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2323
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2325
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2326
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2328
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2329
Product: latitude_3590					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2330
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2331
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2333
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2334
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2336
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2337
Product: latitude_5280					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2339
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2340
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2342
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2343
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2345
Product: latitude_5285_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2346
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2348
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2349
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2351
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2352
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5289					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2354
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2355
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2357
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2358
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2360
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2361
Product: latitude_5290					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2363
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2364
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2366
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2367
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2369
Product: latitude_5290_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2371
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2372
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2374
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2375
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2377
Product: latitude_5300					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2378
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2380
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2381
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2383
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2384
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: latitude_5300_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2386
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2387
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2389
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2390
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2392
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2393
Product: latitude_5310					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2395
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2396
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2398
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2399
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2401
Product: latitude_5310_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2402
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2404
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2405
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2407
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2408
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5400					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2410
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2412
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2413
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2415
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2416
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_5401					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2418
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2419
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2421
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2422
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2424
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2425
Product: latitude_5410					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2427
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2428
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2430
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2431
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2433
Product: latitude_5411					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2434
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2436
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2437
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2439
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2440
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5414_rugged					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2442
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2443
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2445
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2446
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2448
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2449
Product: latitude_5420_rugged					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2450
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2451
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2453
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2454
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2456
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2457
Product: latitude_5480					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2459
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2460
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2462
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2463
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2465
Product: latitude_5488					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2466
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2468
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2469
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2471
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2472
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5490					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2474
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2475
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2477
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2478
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2480
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2481
Product: latitude_5491					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2483
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2484
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2486
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2487
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2489
Product: latitude_5495					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2491
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2492
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2494
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2495
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2497
Product: latitude_5500					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2498
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2500
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2501
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2503
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2504
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: latitude_5501					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2506
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2507
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2509
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2510
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2512
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2513
Product: latitude_5510					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2515
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2516
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2518
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2519
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2521
Product: latitude_5511					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2522
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2524
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2525
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2527
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2528
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5580					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2530
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2532
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2533
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2535
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2536
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_5590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2538
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2539
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2541
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2542
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2544
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2545
Product: latitude_5591					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2547
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2548
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2550
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2551
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2553
Product: latitude_7200_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2554
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2556
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2557
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2559
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2560
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7210_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2562
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2563
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2565
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2566
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2568
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2569
Product: latitude_7212_rugged_extreme_tablet					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2570
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2571
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2573
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2574
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2576
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2577
Product: latitude_7214_rugged_extreme					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2579
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2580
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2582
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2583
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2585
Product: latitude_7220ex_rugged_extreme_tablet					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2586
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2588
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2589
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2591
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2592
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7220_rugged_extreme_tablet					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2594
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2595
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2597
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2598
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2600
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2601
Product: latitude_7275_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2603
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2604
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2606
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2607
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2609
Product: latitude_7290					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2611
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2612
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2614
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2615
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2617
Product: latitude_7300					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2618
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2620
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2621
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2623
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2624
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: latitude_7310					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2626
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2627
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2629
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2630
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2632
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2633
Product: latitude_7370					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2635
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2636
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2638
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2639
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2641
Product: latitude_7380					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2642
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2644
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2645
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2647
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2648
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7389					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2650
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2652
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2653
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2655
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2656
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_7390					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2658
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2659
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2661
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2662
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2664
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2665
Product: latitude_7390_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2667
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2668
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2670
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2671
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2673
Product: latitude_7400					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2674
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2676
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2677
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2679
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2680
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7400_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2682
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2683
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2685
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2686
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2688
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2689
Product: latitude_7410					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2690
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2691
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2693
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2694
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2696
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2697
Product: latitude_7414_rugged_extreme					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2699
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2700
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2702
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2703
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2705
Product: latitude_7424_rugged_extreme					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2706
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2708
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2709
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2711
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2712
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7480					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2714
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2715
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2717
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2718
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2720
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2721
Product: latitude_7490					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2723
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2724
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2726
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2727
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2729
Product: latitude_9410					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2731
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2732
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2734
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2735
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2737
Product: latitude_9510					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2738
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2740
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2741
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2743
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2744
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: latitude_e5270					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2746
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2747
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2749
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2750
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2752
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2753
Product: latitude_e5470					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2755
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2756
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2758
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2759
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2761
Product: latitude_e5570					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2762
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2764
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2765
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2767
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2768
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_e7270					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2770
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2772
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2773
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2775
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2776
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_e7470					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2778
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2779
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2781
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2782
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2784
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-LATI-201022/2785
Product: optiplex_3000_thin_client					
Affected Version(s): -					
Incorrect Comparison	10-Oct-2022	4.9	Dell Wyse ThinOS 2205 contains a Regular Expression Denial of Service Vulnerability in UI. An admin privilege attacker could potentially exploit this vulnerability,	https://www.dell.com/support/kbdoc/en-us/000203376/dsa-2022-247-dell-wyse-thinos-security-update-for-a-regular-	H-DEL-OPTI-201022/2786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to denial-of-service. **CVE ID : CVE-2022-34402**	expression-vulnerability	
Product: optiplex_3040					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2787
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2788
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2790
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2791
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2793
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2794
Product: optiplex_3046					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2796
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2797
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2799
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2800
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2802
Product: optiplex_3050					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2804
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2805
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2807
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2808
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2810
Product: optiplex_3050_aio					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2811
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2813
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2814
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2816
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2817
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: optiplex_3060					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2819
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2820
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2822
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2823
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2825
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2826
Product: optiplex_3070					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2828
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2829
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2831
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2832
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2834
Product: optiplex_3080					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2835
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2837
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2838
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2840
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2841
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_3090					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2843
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2845
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2846
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2848
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2849
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: optiplex_3280_aio					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2851
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2852
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2854
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2855
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2857
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2858
Product: optiplex_5050					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2860
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2861
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2863
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2864
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2866
Product: optiplex_5055					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2867
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2869
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2870
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2872
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2873
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_5060					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2875
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2876
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2878
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2879
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2881
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2882
Product: optiplex_5070					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2883
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2884
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2886
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2887
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2889
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2890
Product: optiplex_5080					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2892
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2893
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2895
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2896
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2898
Product: optiplex_5260_all-in-one					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2899
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2901
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2902
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2904
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2905
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_5480_all-in-one					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2907
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2908
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2910
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2911
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2913
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2914
Product: optiplex_7040					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2916
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2917
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2919
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2920
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2922
Product: optiplex_7050					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2924
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2925
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2927
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2928
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2930
Product: optiplex_7060					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2931
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2933
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2934
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2936
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2937
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: optiplex_7070					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2939
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2940
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2942
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2943
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2945
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2946
Product: optiplex_7070_ultra					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2948
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2949
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2951
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2952
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2954
Product: optiplex_7071					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2955
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2957
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2958
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2960
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2961
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_7080					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2963
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2965
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2966
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2968
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2969
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: optiplex_7450					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2971
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2972
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2974
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2975
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2977
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2978
Product: optiplex_7460_all_in_one					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2980
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2981
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2983
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2984
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2986
Product: optiplex_7470_all-in-one					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2987
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2989
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2990
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2992
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2993
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_7480_all-in-one					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2995
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2996
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2998
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/2999
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3001
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3002
Product: optiplex_xe3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3003
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3004
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3006
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3007
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3009
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-OPTI-201022/3010
Product: precision_3240_compact					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3012
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3013
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3015
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3016
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3018
Product: precision_3420_tower					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3019
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3021
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3022
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3024
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3025
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_3430_tower					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3027
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3028
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3030
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3031
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3033
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3034
Product: precision_3431_tower					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3036
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3037
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3039
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3040
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3042
Product: precision_3440					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3044
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3045
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3047
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3048
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3050
Product: precision_3510					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3051
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3053
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3054
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3056
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3057
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: precision_3520					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3059
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3060
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3062
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3063
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3065
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3066
Product: precision_3540					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3068
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3069
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3071
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3072
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3074
Product: precision_3541					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3075
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3077
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3078
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3080
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3081
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_3550					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3083
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3085
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3086
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3088
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3089
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: precision_3551					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3091
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3092
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3094
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3095
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3097
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3098
Product: precision_3620_tower					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3100
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3101
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3103
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3104
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3106
Product: precision_3630_tower					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3107
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3109
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3110
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3112
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3113
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_3640_tower					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3115
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3116
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3118
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3119
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3121
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3122
Product: precision_3930_rack					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3123
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3124
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3126
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3127
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3129
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3130
Product: precision_5510					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3132
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3133
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3135
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3136
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3138
Product: precision_5530					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3139
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3141
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3142
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3144
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3145
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_5530_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3147
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3148
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3150
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3151
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3153
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3154
Product: precision_5540					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3156
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3157
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3159
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3160
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3162
Product: precision_5720_aio					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3164
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3165
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3167
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3168
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3170
Product: precision_5820_tower					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32486**	https://www.dell.com/support/kbdoc/000202772	H-DEL-PREC-201022/3171
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000202772	H-DEL-PREC-201022/3172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32492		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3173
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3174
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3176
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3177
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3179
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3180
Product: precision_7510					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3182
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3183
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3185
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3186
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3188
Product: precision_7520					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3189
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3191
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3192
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3194
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3195
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_7530					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3197
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3198
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3200
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3201
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3203
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3204
Product: precision_7540					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3205
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3206
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3208
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3209
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3211
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3212
Product: precision_7550					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3214
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3215
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3217
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3218
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3220
Product: precision_7710					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3221
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3223
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3224
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3226
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3227
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_7720					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3229
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3230
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3232
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3233
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3235
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3236
Product: precision_7730					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3238
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3239
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3241
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3242
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3244
Product: precision_7740					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3246
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3247
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3249
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3250
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3252
Product: precision_7750					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3253
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3255
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3256
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3258
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3259
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: precision_7820_tower					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32486**	https://www.dell.com/support/kbdoc/000202772	H-DEL-PREC-201022/3261
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32492**	https://www.dell.com/support/kbdoc/000202772	H-DEL-PREC-201022/3262
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3264
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3265
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3267
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3268
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3270
Product: precision_7920_tower					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32486**	https://www.dell.com/support/kbdoc/000202772	H-DEL-PREC-201022/3271
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000202772	H-DEL-PREC-201022/3272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32492**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3273
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3274
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3276
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3277
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3279
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-PREC-201022/3280
Product: vostro_3070					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3282
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3283
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3285
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3286
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3288
Product: vostro_3267					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3290
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3291
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3293
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3294
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3296
Product: vostro_3268					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3297
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3299
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3300
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3302
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3303
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: vostro_3401					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3305
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3306
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3308
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3309
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3311
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3312
Product: vostro_3470					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3314
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3315
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3317
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3318
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3320
Product: vostro_3471					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3321
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3323
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3324
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3326
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3327
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_3480					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3329
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3331
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3332
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3334
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3335
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: vostro_3481					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3337
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3338
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3340
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3341
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3343
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3344
Product: vostro_3490					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3346
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3347
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3349
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3350
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3352
Product: vostro_3501					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3353
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3355
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3356
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3358
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3359
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_3580					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3361
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3362
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3364
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3365
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3367
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3368
Product: vostro_3581					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3369
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3370
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3372
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3373
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3375
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3376
Product: vostro_3582					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3378
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3379
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3381
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3382
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3384
Product: vostro_3583					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3385
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3387
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3390
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3391
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_3584					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3393
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3394
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3396
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3397
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3399
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3400
Product: vostro_3590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3402
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3403
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3405
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3406
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3408
Product: vostro_3667					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3410
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3411
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3413
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3414
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3416
Product: vostro_3668					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3417
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3419
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3420
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3422
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3423
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: vostro_3669					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3425
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3426
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3428
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3429
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3431
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3432
Product: vostro_3670					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3434
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3435
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3437
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3438
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3440
Product: vostro_3671					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3441
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3443
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3444
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3446
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3447
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_3681					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3449
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3451
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3452
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3454
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3455
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: vostro_3881					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3457
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3458
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3460
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3461
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3463
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3464
Product: vostro_3888					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3466
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3467
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3469
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3470
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3472
Product: vostro_5090					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3473
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3475
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3476
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3478
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3479
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_5390					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3481
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3482
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3484
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3485
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3487
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3488
Product: vostro_5391					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3489
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3490
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3492
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3493
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3495
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3496
Product: vostro_5581					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3498
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3499
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3501
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3502
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3504
Product: vostro_5590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3505
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3507
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3508
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3510
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3511
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_5591					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3513
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3514
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3516
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3517
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3519
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3520
Product: vostro_5880					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3522
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3523
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3525
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3526
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3528
Product: vostro_7590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3530
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3531
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3533
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3534
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-VOST-201022/3536
Product: wyse_3040_thin_client					
Affected Version(s): -					
Incorrect Comparison	10-Oct-2022	4.9	Dell Wyse ThinOS 2205 contains a Regular Expression Denial of Service Vulnerability in UI. An admin privilege attacker could potentially exploit this vulnerability, leading to denial-of-service. **CVE ID : CVE-2022-34402**	https://www.dell.com/support/kbdoc/en-us/000203376/dsa-2022-247-dell-wyse-thinos-security-update-for-a-regular-expression-vulnerability	H-DEL-WYSE-201022/3537
Product: wyse_5070					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3539
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3540
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3542
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3543
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3545
Product: wyse_5070_thin_client					
Affected Version(s): -					
Incorrect Comparison	10-Oct-2022	4.9	Dell Wyse ThinOS 2205 contains a Regular Expression Denial of Service Vulnerability in UI. An admin privilege attacker could potentially exploit this vulnerability, leading to denial-of-service. **CVE ID : CVE-2022-34402**	https://www.dell.com/support/kbdoc/en-us/000203376/dsa-2022-247-dell-wyse-thinos-security-update-for-a-regular-expression-vulnerability	H-DEL-WYSE-201022/3546
Product: wyse_5470					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3548
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3549
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3551
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3552
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3554
Product: wyse_5470_all-in-one					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3555
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation	https://www.dell.com/suppor	H-DEL-WYSE-201022/3556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	t/kbdoc/000203758	
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3557
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3558
Buffer Copy without	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow	https://www.dell.com/suppor	H-DEL-WYSE-201022/3559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	t/kbdoc/000203758	
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3560
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3561
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation	https://www.dell.com/suppor	H-DEL-WYSE-201022/3562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	t/kbdoc/000203758	
Product: wyse_5470_all-in-one_thin_client					
Affected Version(s): -					
Incorrect Comparison	10-Oct-2022	4.9	Dell Wyse ThinOS 2205 contains a Regular Expression Denial of Service Vulnerability in UI. An admin privilege attacker could potentially exploit this vulnerability, leading to denial-of-service. **CVE ID : CVE-2022-34402**	https://www.dell.com/support/kbdoc/en-us/000203376/dsa-2022-247-dell-wyse-thinos-security-update-for-a-regular-expression-vulnerability	H-DEL-WYSE-201022/3563
Product: wyse_5470_mobile_thin_client					
Affected Version(s): -					
Incorrect Comparison	10-Oct-2022	4.9	Dell Wyse ThinOS 2205 contains a Regular Expression Denial of Service Vulnerability in UI. An admin privilege attacker could potentially exploit this vulnerability, leading to denial-of-service. **CVE ID : CVE-2022-34402**	https://www.dell.com/support/kbdoc/en-us/000203376/dsa-2022-247-dell-wyse-thinos-security-update-for-a-regular-expression-vulnerability	H-DEL-WYSE-201022/3564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wyse_7040_thin_client					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3565
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3566
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3568
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3569
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3571
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-WYSE-201022/3572
Product: xps_13_7390					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3574
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3575
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3577
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3578
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3580
Product: xps_13_7390_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3581
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3583
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3584
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3586
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3587
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: xps_13_9300					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3589
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3590
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3592
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3593
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3595
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3596
Product: xps_13_9365_2-in-1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3597
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3598
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3600
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3601
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3603
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3604
Product: xps_13_9370					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3606
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3607
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3609
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3610
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3612
Product: xps_13_9380					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3613
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3615
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3616
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3618
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3619
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: xps_15_7590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3621
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3622
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3625
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3627
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3628
Product: xps_15_9575_2-in-1					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3630
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3631
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3633
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3634
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3636
Product: xps_7590					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3638
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3639
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3641
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3642
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3644
Product: xps_8930					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3645
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3647
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3648
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3650
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3651
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: xps_8940					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3653
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3654
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3656
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3657
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3659
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3660
Product: xps_8950					
Affected Version(s): -					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3662
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3663
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3665
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3666
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	H-DEL-XPS_-201022/3668
Product: xtremio_x1					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	12-Oct-2022	9.8	Dell EMC XtremIO versions prior to X2 6.4.0-22 contain a bruteforce vulnerability. A remote unauthenticated attacker can potentially exploit this vulnerability and gain access to an admin account. **CVE ID : CVE-2022-31228**	https://www.dell.com/support/kbdoc/en-us/000204112/dsa-2022-145-dell-emc-xtremeio-for-ssh-and-web-ui-vulnerability	H-DEL-XTRE-201022/3669
Product: xtremio_x2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	12-Oct-2022	9.8	Dell EMC XtremIO versions prior to X2 6.4.0-22 contain a bruteforce vulnerability. A remote unauthenticated attacker can potentially exploit this vulnerability and gain access to an admin account. **CVE ID : CVE-2022-31228**	https://www.dell.com/support/kbdoc/en-us/000204112/dsa-2022-145-dell-emc-xtremeio-for-ssh-and-web-ui-vulnerability	H-DEL-XTRE-201022/3670
Vendor: foresightsports					
Product: gc3_launch_monitor					
Affected Version(s): -					
Incorrect Default Permissions	13-Oct-2022	8	Foresight GC3 Launch Monitor 1.3.15.68 ships with a Target Communication Framework (TCF) service enabled. This service listens on a TCP port on all interfaces and allows for process debugging, file system modification, and terminal access as the root user. In conjunction with a hosted wireless access point and the known passphrase of FSSPORTS, an attacker could use this service to modify a device and	N/A	H-FOR-GC3_-201022/3671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			steal intellectual property. **CVE ID : CVE-2022-40187**		
Vendor: generex					
Product: cs141					
Affected Version(s): -					
N/A	06-Oct-2022	7.2	Generex CS141 through 2.10 allows remote command execution by administrators via a web interface that reaches run_update in /usr/bin/gxserve-update.sh (e.g., command execution can occur via a reverse shell installed by install.sh). **CVE ID : CVE-2022-42457**	https://www.generex.de/support/downloads/ups/cs141, https://www.generex.de/products/ups/	H-GEN-CS14-201022/3672
Vendor: mediabridgeproducts					
Product: mlwr-ac1200r					
Affected Version(s): -					
Improper Authentication	12-Oct-2022	9.8	A vulnerability classified as critical was found in Mediabridge Medialink. This vulnerability affects unknown code of the file /index.asp. The manipulation leads to improper authentication. The attack can be initiated remotely. The exploit has	N/A	H-MED-MLWR-201022/3673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210700. **CVE ID : CVE-2022-3465**		
Vendor: mediatek					
Product: mt6580					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT65-201022/3674
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT65-201022/3675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**		
Product: mt6739					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3676
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3678
Product: mt6753					
Affected Version(s): -					
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32591		
Product: mt6757					
Affected Version(s): -					
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3680
Product: mt6761					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3682
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3684
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3685
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**		
Product: mt6762					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3687
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3689
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3691
Product: mt6763					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26472		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3693
Product: mt6765					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3695
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3696
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-201022/3697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	bulletin/October-2022	
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3698
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**		
Product: mt6768					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3700
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3702
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3704
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3705
Product: mt6769					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format	https://corp.mediatek.com/product-security-	H-MED-MT67-201022/3706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	bulletin/October-2022	
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3707
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**		
Product: mt6771					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3709
Product: mt6779					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3711
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**		
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3713
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3714
Product: mt6781					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3715
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3716
Improper Resource	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible	https://corp.mediatek.com/pr	H-MED-MT67-201022/3717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	oduct-security-bulletin/October-2022	
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3718
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3720
Product: mt6785					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3722
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3724
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3725
Improper Handling	07-Oct-2022	6.7	In wlan, there is a possible use after	https://corp.mediatek.com/pr	H-MED-MT67-201022/3726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Exceptional Conditions			free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	oduct-security-bulletin/October-2022	
Product: mt6789					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3727
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format	https://corp.mediatek.com/product-security-	H-MED-MT67-201022/3728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	bulletin/October-2022	
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3729
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**		
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3731
Incorrect Calculation of Buffer Size	07-Oct-2022	6.7	In sensorhub, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07129717; Issue ID: ALPS07129717.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26474		
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3733
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT67-201022/3734
Product: mt6833					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3735
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3736
Improper Resource	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an	https://corp.mediatek.com/product-security-	H-MED-MT68-201022/3737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	bulletin/October-2022	
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3738
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**		
Product: mt6853					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3740
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3742
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32591		
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3744
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3745
Product: mt6853t					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3746
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3747
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-201022/3748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	bulletin/October-2022	
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3749
Product: mt6855					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3751
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**		
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3753
Incorrect Calculation of Buffer Size	07-Oct-2022	6.7	In sensorhub, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07129717; Issue ID: ALPS07129717. **CVE ID : CVE-2022-26474**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3755
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3756
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**		
Product: mt6873					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3758
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3760
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**		
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3762
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3763
Product: mt6875					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3764
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3765
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an	https://corp.mediatek.com/product-security-	H-MED-MT68-201022/3766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	bulletin/October-2022	
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3767
Product: mt6877					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3769
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3771
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32590		
Product: mt6879					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3773
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26472		
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3775
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3776
Improper Synchronization	07-Oct-2022	6.7	In isp, there is a possible use after free due to	https://corp.mediatek.com/product-security-	H-MED-MT68-201022/3777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262305; Issue ID: ALPS07262305. **CVE ID : CVE-2022-26452**	bulletin/October-2022	
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3778
Incorrect Calculation of Buffer Size	07-Oct-2022	6.7	In sensorhub, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07129717; Issue ID: ALPS07129717. **CVE ID : CVE-2022-26474**		
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3780
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3782
Product: mt6883					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3783
Deserialization of	07-Oct-2022	7.8	In ims, there is a possible escalation	https://corp.mediatek.com/pr	H-MED-MT68-201022/3784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	oduct-security-bulletin/October-2022	
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3785
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3787
Product: mt6885					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3789
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3791
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3792
Improper Handling	07-Oct-2022	6.7	In wlan, there is a possible use after	https://corp.mediatek.com/pr	H-MED-MT68-201022/3793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Exceptional Conditions			free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	oduct-security-bulletin/October-2022	
Product: mt6889					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3794
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format	https://corp.mediatek.com/product-security-	H-MED-MT68-201022/3795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	bulletin/October-2022	
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3796
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3798
Product: mt6891					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3800
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32590		
Product: mt6893					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3802
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26472		
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3804
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3805
Improper Handling of	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an	https://corp.mediatek.com/product-security-	H-MED-MT68-201022/3806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	bulletin/October-2022	
Product: mt6895					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3807
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3809
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**		
Improper Synchronization	07-Oct-2022	6.7	In isp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262305; Issue ID: ALPS07262305. **CVE ID : CVE-2022-26452**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3811
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation of Buffer Size	07-Oct-2022	6.7	In sensorhub, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07129717; Issue ID: ALPS07129717. **CVE ID : CVE-2022-26474**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3813
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3814
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**		
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT68-201022/3816
Product: mt6983					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3818
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3820
Improper Synchronization	07-Oct-2022	6.7	In isp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262305; Issue ID: ALPS07262305. **CVE ID : CVE-2022-26452**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3821
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to	https://corp.mediatek.com/product-security-	H-MED-MT69-201022/3822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	bulletin/October-2022	
Incorrect Calculation of Buffer Size	07-Oct-2022	6.7	In sensorhub, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07129717; Issue ID: ALPS07129717. **CVE ID : CVE-2022-26474**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3823
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3825
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32592		
Improper Input Validation	07-Oct-2022	6.7	In vowe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138493; Issue ID: ALPS07138493. **CVE ID : CVE-2022-32593**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT69-201022/3827
Product: mt7663					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT76-201022/3828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT76-201022/3829
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT76-201022/3830
Product: mt7668					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an	https://corp.mediatek.com/product-security-	H-MED-MT76-201022/3831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	bulletin/October-2022	
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT76-201022/3832
Product: mt7902					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT79-201022/3833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT79-201022/3834
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT79-201022/3835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**		
Product: mt7921					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT79-201022/3836
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT79-201022/3837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26475		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT79-201022/3838
Product: mt8167s					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3840
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3841
Product: mt8168					
Affected Version(s): -					
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking.	https://corp.mediatek.com/product-security-	H-MED-MT81-201022/3842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	bulletin/October-2022	
Product: mt8175					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3843
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3845
Product: mt8183					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3847
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32590		
Product: mt8185					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3849
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3851
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT81-201022/3852
Product: mt8321					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a	https://corp.mediatek.com/product-security-	H-MED-MT83-201022/3853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	bulletin/October-2022	
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3854
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**		
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3856
Product: mt8362a					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3858
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32590		
Product: mt8365					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3860
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3862
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3863
Product: mt8385					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a	https://corp.mediatek.com/product-security-	H-MED-MT83-201022/3864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	bulletin/October-2022	
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3865
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3867
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3869
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT83-201022/3870
Product: mt8512a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT85-201022/3871
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT85-201022/3872
Improper Handling of Exceptiona	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status	https://corp.mediatek.com/product-security-	H-MED-MT85-201022/3873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	bulletin/October-2022	
Product: mt8518					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT85-201022/3874
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT85-201022/3875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT85-201022/3876
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT85-201022/3877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**		
Product: mt8532					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT85-201022/3878
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT85-201022/3879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26475		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT85-201022/3880
Product: mt8666					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3882
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3883
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**		
Product: mt8667					
Affected Version(s): -					
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3885
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3887
Product: mt8675					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3889
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32591		
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3891
Product: mt8695					
Affected Version(s): -					
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3893
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3894
Product: mt8696					
Affected Version(s): -					
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking.	https://corp.mediatek.com/product-security-	H-MED-MT86-201022/3895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	bulletin/October-2022	
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3896
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT86-201022/3897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**		
Product: mt8765					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3898
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3900
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3901
Product: mt8766					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3902
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3903
Improper Resource	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible	https://corp.mediatek.com/pr	H-MED-MT87-201022/3904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	oduct-security-bulletin/October-2022	
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3905
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3907
Product: mt8768					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3909
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3911
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3912
Improper Handling	07-Oct-2022	6.7	In wlan, there is a possible use after	https://corp.mediatek.com/pr	H-MED-MT87-201022/3913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Exceptional Conditions			free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	oduct-security-bulletin/October-2022	
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3914
Product: mt8786					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3916
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3918
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3920
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3921
Product: mt8788					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3922
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3923
Improper Resource	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible	https://corp.mediatek.com/pr	H-MED-MT87-201022/3924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	oduct-security-bulletin/October-2022	
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3925
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3927
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**		
Product: mt8789					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3929
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3931
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3933
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3934
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**		
Product: mt8791					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3936
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3938
Product: mt8797					
Affected Version(s): -					
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3940
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259;	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**		
Product: mt8798					
Affected Version(s): -					
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	https://corp.mediatek.com/product-security-bulletin/October-2022	H-MED-MT87-201022/3942
Vendor: Microsoft					
Product: storsimple_8010					
Affected Version(s): -					
N/A	11-Oct-2022	6.8	StorSimple 8000 Series Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38017**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38017	H-MIC-STOR-201022/3943
Product: storsimple_8020					
Affected Version(s): -					
N/A	11-Oct-2022	6.8	StorSimple 8000 Series Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	H-MIC-STOR-201022/3944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38017	ory/CVE-2022-38017	
Vendor: Qualcomm					
Product: sm8150					
Affected Version(s): -					
Use After Free	07-Oct-2022	7.8	A use after free vulnerability in perf-mgr driver prior to SMR Oct-2022 Release 1 allows attacker to cause memory access fault. **CVE ID : CVE-2022-39853**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	H-QUA-SM81-201022/3945
Product: sm8250					
Affected Version(s): -					
Use After Free	07-Oct-2022	7.8	A use after free vulnerability in perf-mgr driver prior to SMR Oct-2022 Release 1 allows attacker to cause memory access fault. **CVE ID : CVE-2022-39853**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	H-QUA-SM82-201022/3946
Vendor: Samsung					
Product: exynos					
Affected Version(s): -					
N/A	07-Oct-2022	7.8	Improper protection in IOMMU prior to SMR Oct-2022 Release 1 allows unauthorized access to secure memory.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	H-SAM-EXYN-201022/3947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39854		
Vendor: Siemens					
Product: 6ag1206-2bb00-7ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6AG1-201022/3948
Product: 6ag1206-2bs00-7ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6AG1-201022/3949
Product: 6ag1208-0ba00-7ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6AG1-201022/3950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6ag1216-4bs00-7ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6AG1-201022/3951
Product: 6gk5204-0ba00-2gf2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3952
Product: 6gk5204-0ba00-2yf2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5204-2aa00-2gf2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3954
Product: 6gk5204-2aa00-2yf2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3955
Product: 6gk5205-3bb00-2ab2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/3956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5205-3bb00-2tb2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3957
Product: 6gk5205-3bd00-2ab2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3958
Product: 6gk5205-3bd00-2tb2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3959
Product: 6gk5205-3bf00-2ab2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3960
Product: 6gk5205-3bf00-2tb2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5206-2bb00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3962
Product: 6gk5206-2bd00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3963
Product: 6gk5206-2bs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5206-2bs00-2fc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3965
Product: 6gk5206-2gs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3966
Product: 6gk5206-2gs00-2fc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5206-2gs00-2tc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3968
Product: 6gk5206-2rs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3969
Product: 6gk5206-2rs00-5ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5206-2rs00-5fc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3971
Product: 6gk5208-0ba00-2ab2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3972
Product: 6gk5208-0ba00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/3973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5208-0ba00-2fc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3974
Product: 6gk5208-0ba00-2tb2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3975
Product: 6gk5208-0ga00-2ac2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3976
Product: 6gk5208-0ga00-2fc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3977
Product: 6gk5208-0ga00-2tc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5208-0ha00-2as6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3979
Product: 6gk5208-0ha00-2es6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3980
Product: 6gk5208-0ha00-2ts6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5208-0ra00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3982
Product: 6gk5208-0ra00-5ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3983
Product: 6gk5208-0ua00-5es6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5213-3bb00-2ab2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3985
Product: 6gk5213-3bb00-2tb2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3986
Product: 6gk5213-3bd00-2ab2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5213-3bd00-2tb2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3988
Product: 6gk5213-3bf00-2ab2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3989
Product: 6gk5213-3bf00-2tb2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/3990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5216-0ba00-2ab2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3991
Product: 6gk5216-0ba00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3992
Product: 6gk5216-0ba00-2fc2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3993
Product: 6gk5216-0ba00-2tb2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3994
Product: 6gk5216-0ha00-2as6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5216-0ha00-2es6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3996
Product: 6gk5216-0ha00-2ts6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3997
Product: 6gk5216-0ua00-5es6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5216-3rs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/3999
Product: 6gk5216-3rs00-5ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4000
Product: 6gk5216-4bs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5216-4gs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4002
Product: 6gk5216-4gs00-2fc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4003
Product: 6gk5216-4gs00-2tc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5224-0ba00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4005
Product: 6gk5224-4gs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4006
Product: 6gk5224-4gs00-2fc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/4007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5224-4gs00-2tc2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4008
Product: 6gk5324-0ba00-2ar3					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4009
Product: 6gk5324-0ba00-3ar3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4010
Product: 6gk5326-2qs00-3ar3					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4011
Product: 6gk5326-2qs00-3rr3					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5328-4fs00-2ar3					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4013
Product: 6gk5328-4fs00-2rr3					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4014
Product: 6gk5328-4fs00-3ar3					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5328-4fs00-3rr3					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4016
Product: 6gk5328-4ss00-2ar3					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4017
Product: 6gk5328-4ss00-3ar3					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5408-4gp00-2am2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4019
Product: 6gk5408-4gq00-2am2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4020
Product: 6gk5408-8gr00-2am2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5408-8gs00-2am2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4022
Product: 6gk5416-4gr00-2am2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4023
Product: 6gk5416-4gs00-2am2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/4024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5524-8gr00-2ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4025
Product: 6gk5524-8gr00-3ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4026
Product: 6gk5524-8gr00-4ar2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4027
Product: 6gk5524-8gs00-2ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4028
Product: 6gk5524-8gs00-3ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5524-8gs00-4ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4030
Product: 6gk5526-8gr00-2ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4031
Product: 6gk5526-8gr00-3ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5526-8gr00-4ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4033
Product: 6gk5526-8gs00-2ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4034
Product: 6gk5526-8gs00-3ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5526-8gs00-4ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4036
Product: 6gk5528-0aa00-2ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4037
Product: 6gk5528-0aa00-2hr2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5528-0ar00-2ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4039
Product: 6gk5528-0ar00-2hr2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4040
Product: 6gk5552-0aa00-2ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/4041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5552-0aa00-2hr2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4042
Product: 6gk5552-0ar00-2ar2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4043
Product: 6gk5552-0ar00-2hr2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4044
Product: 6gk5622-2gs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4045
Product: 6gk5632-2gs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5636-2gs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4047
Product: 6gk5642-2gs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4048
Product: 6gk5646-2gs00-2ac2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5721-1fc00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4050
Product: 6gk5721-1fc00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4051
Product: 6gk5722-1fc00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5722-1fc00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4053
Product: 6gk5722-1fc00-0ac0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4054
Product: 6gk5734-1fx00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5734-1fx00-0aa6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4056
Product: 6gk5734-1fx00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4057
Product: 6gk5734-1fx00-0ab6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/4058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5738-1gy00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4059
Product: 6gk5738-1gy00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4060
Product: 6gk5748-1fc00-0aa0					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4061
Product: 6gk5748-1fc00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4062
Product: 6gk5748-1gd00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5748-1gd00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4064
Product: 6gk5748-1gy01-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4065
Product: 6gk5748-1gy01-0ta0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5761-1fc00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4067
Product: 6gk5761-1fc00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4068
Product: 6gk5763-1al00-3aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5763-1al00-3da0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4070
Product: 6gk5763-1al00-7da0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4071
Product: 6gk5766-1ge00-3da0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5766-1ge00-3db0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4073
Product: 6gk5766-1ge00-7da0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4074
Product: 6gk5766-1ge00-7db0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/4075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5766-1ge00-7ta0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4076
Product: 6gk5766-1ge00-7tb0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4077
Product: 6gk5766-1je00-3da0					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4078
Product: 6gk5766-1je00-7da0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4079
Product: 6gk5766-1je00-7ta0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5774-1fx00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4081
Product: 6gk5774-1fx00-0aa6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4082
Product: 6gk5774-1fx00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5774-1fx00-0ab6					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4084
Product: 6gk5774-1fx00-0ac0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4085
Product: 6gk5774-1fy00-0ta0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5774-1fy00-0tb0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4087
Product: 6gk5778-1gy00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4088
Product: 6gk5778-1gy00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5778-1gy00-0ta0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4090
Product: 6gk5778-1gy00-0tb0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4091
Product: 6gk5786-1fc00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/4092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5786-1fc00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4093
Product: 6gk5786-2fc00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4094
Product: 6gk5786-2fc00-0ab0					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4095
Product: 6gk5786-2fc00-0ac0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4096
Product: 6gk5786-2fe00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5786-2fe00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4098
Product: 6gk5786-2hc00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4099
Product: 6gk5786-2hc00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5788-1fc00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4101
Product: 6gk5788-1fc00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4102
Product: 6gk5788-1gd00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5788-1gd00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4104
Product: 6gk5788-1gy01-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4105
Product: 6gk5788-2fc00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5788-2fc00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4107
Product: 6gk5788-2fc00-0ac0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4108
Product: 6gk5788-2gd00-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/4109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5788-2gd00-0ab0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4110
Product: 6gk5788-2gd00-0ta0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4111
Product: 6gk5788-2gd00-0tb0					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4112
Product: 6gk5788-2gd00-0tc0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4113
Product: 6gk5788-2gy01-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5788-2gy01-0ta0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4115
Product: 6gk5788-2hy01-0aa0					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4116
Product: 6gk5804-0ap00-2aa2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5812-1aa00-2aa2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4118
Product: 6gk5812-1ba00-2aa2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4119
Product: 6gk5816-1aa00-2aa2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5816-1ba00-2aa2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4121
Product: 6gk5826-2ab00-2ab2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4122
Product: 6gk5853-2ea00-2da1					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5856-2ea00-3aa1					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4124
Product: 6gk5856-2ea00-3da1					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4125
Product: 6gk5874-2aa00-2aa2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	H-SIE-6GK5-201022/4126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5874-3aa00-2aa2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4127
Product: 6gk5876-3aa02-2ba2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4128
Product: 6gk5876-3aa02-2ea2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4129
Product: 6gk5876-4aa00-2ba2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4130
Product: 6gk5876-4aa00-2da2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK5-201022/4131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk6108-4am00-2ba2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK6-201022/4132
Product: 6gk6108-4am00-2da2					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	H-SIE-6GK6-201022/4133
Product: 7kg8500-0aa00-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8500-0aa00-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productce	H-SIE-7KG8-201022/4136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
/Argument Delimiters			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All	rt/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8500-0aa10-0aa0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8500-0aa10-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8500-0aa30-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8500-0aa30-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa01-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa01-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa02-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in	https://cert-portal.siemens.	H-SIE-7KG8-201022/4151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	com/productcert/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa02-2aa0					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa11-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa11-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa12-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa12-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa31-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa31-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in	https://cert-portal.siemens.	H-SIE-7KG8-201022/4165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	com/productcert/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa32-0aa0					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa32-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa00-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa00-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa10-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa10-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa30-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in	https://cert-portal.siemens.	H-SIE-7KG8-201022/4179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	com/productcert/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa30-2aa0					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa01-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa01-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa02-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa02-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa11-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa11-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in	https://cert-portal.siemens.	H-SIE-7KG8-201022/4193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	com/productcert/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa12-0aa0					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa12-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa31-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa31-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa32-0aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa32-2aa0					
Affected Version(s): -					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	H-SIE-7KG8-201022/4205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: apogee_modular_building_controller					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.	H-SIE-APOG-201022/4206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	com/productcert/pdf/ssa-313313.pdf	
Product: apogee_modular_equiment_controller					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-APOG-201022/4207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: apogee_pxc_compact					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-APOG-201022/4208
Product: apogee_pxc_modular					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-APOG-201022/4209
Product: desigo_pxc00-e.d					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxc00-u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxc001-e.d					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4212
Product: desigo_pxc100-e.d					
Affected Version(s): -					
Missing Release of Memory after	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf,	H-SIE-DESI-201022/4213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	
Product: desigo_pxc12-e.d					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxc128-u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4215
Product: desigo_pxc200-e.d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4216
Product: desigo_pxc22-e.d					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxc22.1-e.d					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxc36.1-e.d					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4219
Product: desigo_pxc50-e.d					
Affected Version(s): -					
Missing Release of Memory after	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf,	H-SIE-DESI-201022/4220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	
Product: desigo_pxc64-u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxm20-e					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-DESI-201022/4222
Product: desigo_pxm30-1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation"	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41).	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40178		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: desigo_pxm30.e					
Affected Version(s): -					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41).	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A Cross-Site Request Forgery exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40176		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: desigo_pxm40-1					
Affected Version(s): -					
Execution with Unnecessa	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1	https://cert-portal.siemens.com/productce	H-SIE-DESI-201022/4237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ry Privileges			(All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation” web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the “Import Files“ functionality of the “Operation” web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the “Import Files“ functionality of the “Operation” web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: desigo_pxm40.e					
Affected Version(s): -					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: desigo_pxm50-1					
Affected Version(s): -					
Execution with Unnecessa	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productce	H-SIE-DESI-201022/4251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ry Privileges			Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation” web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request	11-Oct-2022	5.3	A vulnerability has been identified in	https://cert-portal.siemens.	H-SIE-DESI-201022/4257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the “Import Files“ functionality of the “Operation” web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload	com/productcert/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: desigo_pxm50.e					
Affected Version(s): -					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation”	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Informatio	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1	https://cert-portal.siemens.com/productce	H-SIE-DESI-201022/4262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to an Unauthorized Actor			(All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-DESI-201022/4264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: logo\!8_bm					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	11-Oct-2022	9.8	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not properly validate the	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	H-SIE-LOGO-201022/4265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			structure of TCP packets in several methods. This could allow an attacker to cause buffer overflows, get control over the instruction counter and run custom code. **CVE ID : CVE-2022-36361**		
Insufficient Verification of Data Authenticity	11-Oct-2022	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). Affected devices load firmware updates without checking the authenticity. Furthermore the integrity of the unencrypted firmware is only verified by a non-cryptographic method. This could allow an attacker to manipulate a firmware update and flash it to the device. **CVE ID : CVE-2022-36360**	https://cert-portal.siemens.com/productcert/pdf/ssa-928782.pdf	H-SIE-LOGO-201022/4266
N/A	11-Oct-2022	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not conduct certain	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	H-SIE-LOGO-201022/4267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validations when interacting with them. This could allow an unauthenticated remote attacker to manipulate the devices IP address, which means the device would not be reachable and could only be recovered by power cycling the device. **CVE ID : CVE-2022-36362**		
Improper Input Validation	11-Oct-2022	5.3	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not properly validate an offset value which can be defined in TCP packets when calling a method. This could allow an attacker to retrieve parts of the content of the memory. **CVE ID : CVE-2022-36363**	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	H-SIE-LOGO-201022/4268
Product: logo\!8_bm_fs-05					
Affected Version(s): -					
Buffer Copy without Checking Size of	11-Oct-2022	9.8	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions).	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	H-SIE-LOGO-201022/4269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Affected devices do not properly validate the structure of TCP packets in several methods. This could allow an attacker to cause buffer overflows, get control over the instruction counter and run custom code. **CVE ID : CVE-2022-36361**		
Insufficient Verification of Data Authenticity	11-Oct-2022	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). Affected devices load firmware updates without checking the authenticity. Furthermore the integrity of the unencrypted firmware is only verified by a non-cryptographic method. This could allow an attacker to manipulate a firmware update and flash it to the device. **CVE ID : CVE-2022-36360**	https://cert-portal.siemens.com/productcert/pdf/ssa-928782.pdf	H-SIE-LOGO-201022/4270
N/A	11-Oct-2022	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants)	https://cert-portal.siemens.com/productce	H-SIE-LOGO-201022/4271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions). Affected devices do not conduct certain validations when interacting with them. This could allow an unauthenticated remote attacker to manipulate the devices IP address, which means the device would not be reachable and could only be recovered by power cycling the device. **CVE ID : CVE-2022-36362**	rt/pdf/ssa-955858.pdf	
Improper Input Validation	11-Oct-2022	5.3	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not properly validate an offset value which can be defined in TCP packets when calling a method. This could allow an attacker to retrieve parts of the content of the memory. **CVE ID : CVE-2022-36363**	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	H-SIE-LOGO-201022/4272
Product: pxg3.w100-1					
Affected Version(s): -					
Execution with	11-Oct-2022	8.8	A vulnerability has been identified in	https://cert-portal.siemens.	H-SIE-PXG3-201022/4273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unnecessary Privileges			Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of	com/productcert/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation” web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the “Import Files“ functionality of the “Operation” web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: pxg3.w100-2					
Affected Version(s): -					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: pxg3.w200-1					
Affected Version(s): -					
Execution with Unnecessa	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productce	H-SIE-PXG3-201022/4287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ry Privileges			Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation” web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request	11-Oct-2022	5.3	A vulnerability has been identified in	https://cert-portal.siemens.	H-SIE-PXG3-201022/4293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload	com/productcert/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: pxg3.w200-2					
Affected Version(s): -					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation”	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Informatio	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1	https://cert-portal.siemens.com/productce	H-SIE-PXG3-201022/4298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to an Unauthorized Actor			(All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	H-SIE-PXG3-201022/4300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: ruggedcom_rm1224					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G)	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-RUGG-201022/4301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m804pb					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31766		
Product: scalance_m812-1					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m816-1					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m826-2					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m874-2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m874-3					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m876-3					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m876-4					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_mum853-1					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_mum856-1					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_s615					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G)	https://cert-portal.siemens.com/productce	H-SIE-SCAL-201022/4312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE	rt/pdf/ssa-697140.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_wam763-1					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_wam766-1					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_wum763-1					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G)	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_wum766-1					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	H-SIE-SCAL-201022/4316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31766		
Product: scalance_x200-4p_irt					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x201-3p_irt					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x201-3p_irt_pro					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x202-2irt					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x202-2p_irt					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x202-2p_irt_pro					
Affected Version(s): -					
Improper Neutralization of Input	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions	https://cert-portal.siemens.com/productce	H-SIE-SCAL-201022/4322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			< V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2	rt/pdf/ssa-501891.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40631		
Product: scalance_x204-2					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204-2fm					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204-2ld					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204-2ld_ts					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204-2ts					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204irt					
Affected Version(s): -					
Improper Neutralization of Input	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions	https://cert-portal.siemens.com/productce	H-SIE-SCAL-201022/4328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			< V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2	rt/pdf/ssa-501891.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40631		
Product: scalance_x204irt_pro					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x206-1					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x206-1ld					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x208					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x208pro					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x212-2					
Affected Version(s): -					
Improper Neutralization of Input	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions	https://cert-portal.siemens.com/productce	H-SIE-SCAL-201022/4334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			< V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2	rt/pdf/ssa-501891.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40631		
Product: scalance_x212-2ld					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x216					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x224					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf201-3p_irt					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf202-2p_irt					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf204					
Affected Version(s): -					
Improper Neutralization of Input	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions	https://cert-portal.siemens.com/productce	H-SIE-SCAL-201022/4340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			< V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2	rt/pdf/ssa-501891.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40631		
Product: scalance_xf204-2					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf204-2ba_irt					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf204irt					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf206-1					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf208					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SCAL-201022/4345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: simatic_drive_controller_cpu_1504d_tf					
Affected Version(s): -					
Insufficiently	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family	https://cert-portal.siemens.com/productce	H-SIE-SIMA-201022/4346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			(All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_drive_controller_cpu_1507d_tf					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_et_200_open_controller_cpu_1515sp_pc					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_et_200_open_controller_cpu_1515sp_pc2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_hmi_comfort_panels					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	H-SIE-SIMA-201022/4350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_hmi_ktp1200_basic					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	H-SIE-SIMA-201022/4351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_hmi_ktp400_basic					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	H-SIE-SIMA-201022/4352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_hmi_ktp700_basic					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	H-SIE-SIMA-201022/4353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_hmi_ktp900_basic					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS	https://cert-portal.siemens.com/productce	H-SIE-SIMA-201022/4354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device	rt/pdf/ssa-384224.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_hmi_ktp_mobile_panels					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	H-SIE-SIMA-201022/4355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_s7-1200_cpu_12_1211c					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1212c					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1212fc					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1214c					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1214fc					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1215c					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions <	https://cert-portal.siemens.com/productce	H-SIE-SIMA-201022/4361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication.	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1215fc					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1217c					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1510sp					
Affected Version(s): -					
Insufficiently	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive	https://cert-portal.siemens.com/productce	H-SIE-SIMA-201022/4364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1510sp-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9),	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1511-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1511t-1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1511tf-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1512c-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: simatic_s7-1500_cpu_1512sp-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1512spf-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1513-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38465		
Product: simatic_s7-1500_cpu_1513f-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1513r-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1515-2					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_151511c-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_151511f-1					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1515f-2					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1515r-2					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1515t-2					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions <	https://cert-portal.siemens.com/productce	H-SIE-SIMA-201022/4380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication.	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1516-3					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1516f-3					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1516pro_f					
Affected Version(s): -					
Insufficiently	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive	https://cert-portal.siemens.com/productce	H-SIE-SIMA-201022/4383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1516t-3					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9),	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1516tf-3					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1517-3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1517f-3					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1518-4					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: simatic_s7-1500_cpu_1518f-4					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1518hf-4					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1518t-4					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38465		
Product: simatic_s7-1500_cpu_1518tf-4					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_15pro-2					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_15prof-2					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-plcsim_advanced					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	H-SIE-SIMA-201022/4395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: siplus_hmi_ktp1200_basic					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	H-SIE-SIPL-201022/4396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: siplus_hmi_ktp400_basic					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	H-SIE-SIPL-201022/4397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: siplus_hmi_ktp700_basic					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	H-SIE-SIPL-201022/4398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: siplus_hmi_ktp900_basic					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4),	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	H-SIE-SIPL-201022/4399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: siplus_net_scalance_x202-2p_irt					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	H-SIE-SIPL-201022/4400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: talon_tc_compact					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	H-SIE-TALO-201022/4401
Vendor: Tenda					
Product: ac1206					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 was discovered to contain a stack overflow via the function formWifiBasicSet. **CVE ID : CVE-2022-42079**	N/A	H-TEN-AC12-201022/4402
Out-of-bounds Write	12-Oct-2022	7.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 was discovered to contain a heap overflow via sched_start_time parameter. **CVE ID : CVE-2022-42080**	N/A	H-TEN-AC12-201022/4403
Out-of-bounds Write	12-Oct-2022	7.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 was discovered to contain a stack overflow via sched_end_time parameter. **CVE ID : CVE-2022-42081**	N/A	H-TEN-AC12-201022/4404
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 is vulnerable to Cross Site Request Forgery (CSRF) via function	N/A	H-TEN-AC12-201022/4405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fromSysToolReboot . **CVE ID : CVE-2022-42077**		
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolRestoreSet. **CVE ID : CVE-2022-42078**	N/A	H-TEN-AC12-201022/4406
Product: ax1803					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 is vulnerable to Cross Site Request Forgery (CSRF) via function TendaAteMode. **CVE ID : CVE-2022-42086**	N/A	H-TEN-AX18-201022/4407
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolReboot . **CVE ID : CVE-2022-42087**	N/A	H-TEN-AX18-201022/4408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): v2					
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 is vulnerable to Cross Site Request Forgery (CSRF) via function TendaAteMode. **CVE ID : CVE-2022-42086**	N/A	H-TEN-AX18-201022/4409
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolReboot. **CVE ID : CVE-2022-42087**	N/A	H-TEN-AX18-201022/4410
Vendor: totolink					
Product: nr1800x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Oct-2022	9.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain a command injection vulnerability via the UploadFirmwareFile function at /cgi-bin/cstecgi.cgi. **CVE ID : CVE-2022-41518**	N/A	H-TOT-NR18-201022/4411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Oct-2022	9.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an unauthenticated stack overflow via the "main" function. **CVE ID : CVE-2022-41522**	N/A	H-TOT-NR18-201022/4412
Out-of-bounds Write	06-Oct-2022	9.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain a command injection vulnerability via the OpModeCfg function at /cgi-bin/cstecgi.cgi. **CVE ID : CVE-2022-41525**	N/A	H-TOT-NR18-201022/4413
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain a stack overflow in the lang parameter in the setLanguageCfg function **CVE ID : CVE-2022-41517**	N/A	H-TOT-NR18-201022/4414
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an	N/A	H-TOT-NR18-201022/4415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated stack overflow via the File parameter in the UploadCustomModule function. **CVE ID : CVE-2022-41520**		
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the sPort/ePort parameter in the setIpPortFilterRules function. **CVE ID : CVE-2022-41521**	N/A	H-TOT-NR18-201022/4416
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the command parameter in the setTracerouteCfg function. **CVE ID : CVE-2022-41523**	N/A	H-TOT-NR18-201022/4417
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an	N/A	H-TOT-NR18-201022/4418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated stack overflow via the week, sTime, and eTime parameters in the setParentalRules function. **CVE ID : CVE-2022-41524**		
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the ip parameter in the setDiagnosisCfg function. **CVE ID : CVE-2022-41526**	N/A	H-TOT-NR18-201022/4419
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the pppoeUser parameter in the setOpModeCfg function. **CVE ID : CVE-2022-41527**	N/A	H-TOT-NR18-201022/4420
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an	N/A	H-TOT-NR18-201022/4421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated stack overflow via the text parameter in the setSmsCfg function. **CVE ID : CVE-2022-41528**		
Vendor: wayos					
Product: lq-04					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**	N/A	H-WAY-LQ-0-201022/4422
Product: lq-05					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the	N/A	H-WAY-LQ-0-201022/4423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**		
Product: lq-06					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**	N/A	H-WAY-LQ-0-201022/4424
Product: lq-07					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the	N/A	H-WAY-LQ-0-201022/4425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server from the affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**		
Product: lq-08					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**	N/A	H-WAY-LQ-0-201022/4426
Product: lq-09					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted	N/A	H-WAY-LQ-0-201022/4427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests to the server from the affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**		
Vendor: wijungle					
Product: u250					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	12-Oct-2022	9.8	WiJungle NGFW Version U250 was discovered to be vulnerable to No Rate Limit attack, allowing the attacker to brute force the admin password leading to Account Take Over. **CVE ID : CVE-2022-33106**	N/A	H-WIJ-U250-201022/4428
Operating System					
Vendor: Apple					
Product: macos					
Affected Version(s): -					
N/A	12-Oct-2022	7.5	Multiple Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aerdl.dll unpacker handler	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/	O-APP-MACO-211022/4429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function crashes. This can lead to a possible scanning engine crash. **CVE ID : CVE-2022-28887**	en/support/security-advisories	
Vendor: arraynetworks					
Product: arrayos_ag					
Affected Version(s): * Up to (including) 9.4.0.469					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Oct-2022	9.8	Array Networks AG/vxAG with ArrayOS AG before 9.4.0.469 allows unauthenticated command injection that leads to privilege escalation and control of the system. NOTE: ArrayOS AG 10.x is unaffected. **CVE ID : CVE-2022-42897**	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/documentation/FieldNotice/Array_Networks_Security_Advisory_Remote_Injection_Vulnerability_in_Array_VPN_Product_ID-11961_%20V2.1.pdf	O-ARR-ARRA-211022/4430
Vendor: Arubanetworks					
Product: arubaos					
Affected Version(s): From (including) 10.3.0.0 Up to (excluding) 10.3.1.1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37885**		
Buffer Copy without Checking Size of Input ('Classic	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37886**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address these security vulnerabilities. **CVE ID : CVE-2022-37887**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x:	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37889**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37891**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Oct-2022	7.8	An authenticated command injection vulnerability exists in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerability. **CVE ID : CVE-2022-37893**		
N/A	07-Oct-2022	6.5	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37894**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	6.1	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37896		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	5.4	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address this	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerability. **CVE ID : CVE-2022-37892**		
N/A	07-Oct-2022	4.9	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37895**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-ARUB-211022/4442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: instant					
Affected Version(s): From (including) 6.4.0.0 Up to (excluding) 6.4.4.8-4.2.4.21					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37885**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37886**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37887**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37889**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37891**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Oct-2022	7.8	An authenticated command injection vulnerability exists in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37893**		
N/A	07-Oct-2022	6.5	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37894**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	6.1	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37896**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	5.4	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address this security vulnerability. **CVE ID : CVE-2022-37892**		
N/A	07-Oct-2022	4.9	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37895**		
Affected Version(s): From (including) 6.5.0.0 Up to (excluding) 6.5.4.24					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37885**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37886**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37887**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Buffer Copy without Checking Size of Input	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37889**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37890**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4460
Buffer Copy without Checking Size of	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37891**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Oct-2022	7.8	An authenticated command injection vulnerability exists in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of this	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37893**		
N/A	07-Oct-2022	6.5	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37894**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	6.1	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37896**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	5.4	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address this security vulnerability. **CVE ID : CVE-2022-37892**		
N/A	07-Oct-2022	4.9	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37895**		
Affected Version(s): From (including) 8.10.0.0 Up to (excluding) 8.10.0.2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37885**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37886**		
Buffer Copy without Checking Size of Input ('Classic	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37887**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x:	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37889**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37891		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Oct-2022	7.8	An authenticated command injection vulnerability exists in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37893**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Oct-2022	6.5	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37894**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4475
Improper Neutralization of Input During	07-Oct-2022	6.1	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			interface could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37896**		
Improper Neutralization of Input	07-Oct-2022	5.4	A vulnerability in the Aruba InstantOS and ArubaOS 10 web	https://www.arubanetworks.com/assets/aler	O-ARU-INST-211022/4477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address this security vulnerability. **CVE ID : CVE-2022-37892**	t/ARUBA-PSA-2022-014.txt	
N/A	07-Oct-2022	4.9	An unauthenticated Denial of Service	https://www.arubanetworks.c	O-ARU-INST-211022/4478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37895**	om/assets/alert/ARUBA-PSA-2022-014.txt	
Affected Version(s): From (including) 8.6.0.0 Up to (excluding) 8.6.0.19					
Buffer Copy without Checking Size of Input	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37885**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address these security vulnerabilities. **CVE ID : CVE-2022-37886**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x:	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37887**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37889**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37891**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Oct-2022	7.8	An authenticated command injection vulnerability exists in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37893**		
N/A	07-Oct-2022	6.5	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address this security vulnerability. **CVE ID : CVE-2022-37894**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	6.1	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37896**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	5.4	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba has released upgrades for Aruba InnstantOS that address this security vulnerability. **CVE ID : CVE-2022-37892**		
N/A	07-Oct-2022	4.9	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerability. **CVE ID : CVE-2022-37895**		
Affected Version(s): From (including) 8.7.0.0 Up to (excluding) 8.7.1.10					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x:	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37885**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37886**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37887**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of these vulnerabilities	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37889**		
Buffer Copy without Checking Size of Input ('Classic	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Successful exploitation results in the execution of arbitrary commands on the underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Oct-2022	9.8	Unauthenticated buffer overflow vulnerabilities exist within the Aruba InstantOS and ArubaOS 10 web management interface. Successful exploitation results in the execution of arbitrary commands on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address these security vulnerabilities. **CVE ID : CVE-2022-37891**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Oct-2022	7.8	An authenticated command injection vulnerability exists in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system of Aruba InstantOS	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37893**		
N/A	07-Oct-2022	6.5	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37894**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	6.1	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37896**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-2022	5.4	A vulnerability in the Aruba InstantOS and ArubaOS 10 web management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below; Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InnstantOS that address this security vulnerability. **CVE ID : CVE-2022-37892**		
N/A	07-Oct-2022	4.9	An unauthenticated Denial of Service (DoS) vulnerability exists in the handling of certain SSID strings by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected AP of Aruba InstantOS 6.4.x: 6.4.4.8-4.2.4.20 and below; Aruba InstantOS 6.5.x: 6.5.4.23 and below; Aruba InstantOS 8.6.x: 8.6.0.18 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.txt	O-ARU-INST-211022/4502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba InstantOS 8.7.x: 8.7.1.9 and below; Aruba InstantOS 8.10.x: 8.10.0.1 and below; ArubaOS 10.3.x: 10.3.1.0 and below; Aruba has released upgrades for Aruba InstantOS that address this security vulnerability. **CVE ID : CVE-2022-37895**		
Vendor: bushnellgolf					
Product: launch_pro_firmware					
Affected Version(s): * Up to (excluding) 1.5.0.2					
Incorrect Default Permissions	13-Oct-2022	8	Foresight GC3 Launch Monitor 1.3.15.68 ships with a Target Communication Framework (TCF) service enabled. This service listens on a TCP port on all interfaces and allows for process debugging, file system modification, and terminal access as the root user. In conjunction with a hosted wireless access point and the known passphrase of FSSPORTS, an attacker could use this service to	N/A	O-BUS-LAUN-211022/4503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modify a device and steal intellectual property. **CVE ID : CVE-2022-40187**		
Vendor: Cisco					
Product: ios					
Affected Version(s): -					
Improper Handling of Exceptional Conditions	10-Oct-2022	7.7	A vulnerability in the SSH implementation of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. This vulnerability is due to improper handling of resources during an exceptional situation. An attacker could exploit this vulnerability by continuously connecting to an affected device and sending specific SSH requests. A successful exploit could allow the attacker to cause the affected device to reload. **CVE ID : CVE-2022-20920**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssh-excpt-dos-FzOBQTnk	O-CIS-IOS-211022/4504
Product: ios_xe					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	10-Oct-2022	8.6	A vulnerability in the DNS application layer gateway (ALG) functionality that is used by Network Address Translation (NAT) in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. This vulnerability is due to a logic error that occurs when an affected device inspects certain TCP DNS packets. An attacker could exploit this vulnerability by sending crafted DNS packets through the affected device that is performing NAT for DNS packets. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition on the affected device. Note: This vulnerability can be exploited only by sending IPv4 TCP packets through an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-alg-dos-KU9Z8kFX	O-CIS-IOS_-211022/4505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability cannot be exploited by sending IPv6 traffic. **CVE ID : CVE-2022-20837**		
N/A	10-Oct-2022	8.6	A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2022-20870**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3	O-CIS-IOS_-211022/4506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	10-Oct-2022	7.7	A vulnerability in the SSH implementation of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. This vulnerability is due to improper handling of resources during an exceptional situation. An attacker could exploit this vulnerability by continuously connecting to an affected device and sending specific SSH requests. A successful exploit could allow the attacker to cause the affected device to reload. **CVE ID : CVE-2022-20920**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssh-excpt-dos-FzOBQTnk	O-CIS-IOS_-211022/4507
Interpretation Conflict	10-Oct-2022	7.4	A vulnerability in the implementation of IPv6 VPN over MPLS (6VPE) with Zone-Based Firewall (ZBFW) of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-6vpe-dos-tJBtf5Zv	O-CIS-IOS_-211022/4508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper error handling of an IPv6 packet that is forwarded from an MPLS and ZBFW-enabled interface in a 6VPE deployment. An attacker could exploit this vulnerability by sending a crafted IPv6 packet sourced from a device on the IPv6-enabled virtual routing and forwarding (VRF) interface through the affected device. A successful exploit could allow the attacker to reload the device, resulting in a DoS condition. **CVE ID : CVE-2022-20915**		
Improper Verification of Cryptographic Signature	10-Oct-2022	6.8	A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q	O-CIS-IOS_-211022/4509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available. **CVE ID : CVE-2022-20944**		
Product: ios_xe_rom_monitor					
Affected Version(s): -					
N/A	10-Oct-2022	4.6	A vulnerability in the password-recovery disable feature of Cisco IOS XE ROM Monitor (ROMMON) Software for Cisco Catalyst Switches could allow an unauthenticated, local attacker to recover the configuration or reset the enable password. This vulnerability is due to a problem with the file and boot variable permissions in ROMMON. An attacker could exploit this vulnerability by rebooting the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO	O-CIS-IOS_-211022/4510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switch into ROMMON and entering specific commands through the console. A successful exploit could allow the attacker to read any file or reset the enable password. **CVE ID : CVE-2022-20864**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
NULL Pointer Dereference	07-Oct-2022	7.5	In ISC DHCP 4.4.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1, when the function option_code_hash_lookup() is called from add_option(), it increases the option's refcount field. However, there is not a corresponding call to option_dereference() to decrement the refcount field. The function add_option() is only used in server responses to lease query packets. Each lease query response calls this function for several options, so eventually, the	https://kb.isc.org/docs/cve-2022-2928	O-DEB-DEBI-211022/4511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reference counters could overflow and cause the server to abort. **CVE ID : CVE-2022-2928**		
Allocation of Resources Without Limits or Throttling	07-Oct-2022	6.5	In ISC DHCP 1.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1 a system with access to a DHCP server, sending DHCP packets crafted to include fqdn labels longer than 63 bytes, could eventually cause the server to run out of memory. **CVE ID : CVE-2022-2929**	https://kb.isc.org/docs/cve-2022-2929	O-DEB-DEBI-211022/4512
Affected Version(s): 11.0					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	11-Oct-2022	6.3	LibreOffice supports Office URI Schemes to enable browser integration of LibreOffice with MS SharePoint server. An additional scheme 'vnd.libreoffice.command' specific to LibreOffice was added. In the affected versions of LibreOffice links using that scheme could be constructed to call internal macros	https://www.libreoffice.org/about-us/security/advisories/CVE-2022-3140	O-DEB-DEBI-211022/4513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with arbitrary arguments. Which when clicked on, or activated by document events, could result in arbitrary script execution without warning. This issue affects: The Document Foundation LibreOffice 7.4 versions prior to 7.4.1; 7.3 versions prior to 7.3.6. **CVE ID : CVE-2022-3140**		
Vendor: Dell					
Product: alienware_area-51_r4_firmware					
Affected Version(s): * Up to (excluding) 2.0.6					
Use of Uninitialized Resource	12-Oct-2022	7.8	Dell BIOS contains a use of uninitialized variable vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-34390**	https://www.dell.com/support/kbdoc/000203882	O-DEL-ALIE-211022/4514
N/A	12-Oct-2022	7.8	Dell Client BIOS Versions prior to the remediated version contain an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203882	O-DEL-ALIE-211022/4515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-34391**		
Product: alienware_area-51_r5_firmware					
Affected Version(s): * Up to (excluding) 2.0.6					
Use of Uninitialized Resource	12-Oct-2022	7.8	Dell BIOS contains a use of uninitialized variable vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-34390**	https://www.dell.com/support/kbdoc/000203882	O-DEL-ALIE-211022/4516
N/A	12-Oct-2022	7.8	Dell Client BIOS Versions prior to the remediated version contain an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203882	O-DEL-ALIE-211022/4517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34391		
Product: alienware_area_51m_r1_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4518
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4519
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4521
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4522
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4524
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4525
Product: alienware_area_51m_r2_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4527
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4528
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4530
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4531
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4533
Product: alienware_aurora_r10_firmware					
Affected Version(s): * Up to (excluding) 2.3.1					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4534
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4536
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4537
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4539
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4540
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: alienware_aurora_r11_firmware					
Affected Version(s): * Up to (excluding) 1.0.16					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4542
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4544
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4545
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4547
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4548
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: alienware_aurora_r12_firmware					
Affected Version(s): * Up to (excluding) 1.1.16					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4550
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4551
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4553
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4554
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4556
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4557
Product: alienware_aurora_r13_firmware					
Affected Version(s): * Up to (excluding) 1.5.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4559
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4560
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4562
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4563
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4565
Product: alienware_aurora_r8_firmware					
Affected Version(s): * Up to (excluding) 1.0.23					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4566
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4568
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4569
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4571
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4572
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: alienware_aurora_r9_firmware					
Affected Version(s): * Up to (excluding) 1.0.20					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4574
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4575
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4577
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4578
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4580
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4581
Product: alienware_m15_r1_firmware					
Affected Version(s): * Up to (excluding) 2.14.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4582
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4583
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4585
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4586
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4588
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4589
Product: alienware_m15_r2_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4591
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4592
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4594
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4595
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4597
Product: alienware_m15_r3_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4598
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4600
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4601
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4603
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4604
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: alienware_m15_r4_firmware					
Affected Version(s): * Up to (excluding) 1.13.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4606
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4607
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4609
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4610
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4612
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4613
Product: alienware_m17_r1_firmware					
Affected Version(s): * Up to (excluding) 2.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4615
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4616
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4618
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4619
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4621
Product: alienware_m17_r2_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4623
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4624
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4626
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4627
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4629
Product: alienware_m17_r3_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4630
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4632
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4633
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4635
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4636
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: alienware_m17_r4_firmware					
Affected Version(s): * Up to (excluding) 1.13.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4638
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4639
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4641
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4642
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4644
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4645
Product: alienware_x14_firmware					
Affected Version(s): * Up to (excluding) 1.5.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4647
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4648
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4650
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4651
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4653
Product: alienware_x15_r1_firmware					
Affected Version(s): * Up to (excluding) 1.11.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4654
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4656
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4657
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4659
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4660
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: alienware_x15_r2_firmware					
Affected Version(s): * Up to (excluding) 1.7.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4662
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4664
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4665
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4667
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4668
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: alienware_x17_r1_firmware					
Affected Version(s): * Up to (excluding) 1.11.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4670
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4671
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4673
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4674
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4676
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4677
Product: alienware_x17_r2_firmware					
Affected Version(s): * Up to (excluding) 1.7.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4679
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4680
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4682
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4683
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-ALIE-211022/4685
Product: bios					
Affected Version(s): * Up to (excluding) 2.21.0					
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32486**	https://www.dell.com/support/kbdoc/000202772	O-DEL-BIOS-211022/4686
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000202772	O-DEL-BIOS-211022/4687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32492**		
Affected Version(s): * Up to (excluding) 2.25.0					
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32486**	https://www.dell.com/support/kbdoc/000202772	O-DEL-BIOS-211022/4688
Improper Input Validation	11-Oct-2022	8.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32492**	https://www.dell.com/support/kbdoc/000202772	O-DEL-BIOS-211022/4689
Product: chengming_3980_firmware					
Affected Version(s): * Up to (excluding) 2.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation	https://www.dell.com/suppor	O-DEL-CHEN-211022/4690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	t/kbdoc/000203758	
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4691
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4692
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation	https://www.dell.com/suppor	O-DEL-CHEN-211022/4693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	t/kbdoc/000203758	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4694
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4695
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation	https://www.dell.com/suppor	O-DEL-CHEN-211022/4696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	t/kbdoc/000203758	
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4697
Product: chengming_3988_firmware					
Affected Version(s): * Up to (excluding) 1.11.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4699
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4700
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4702
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4703
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4705
Product: chengming_3990_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4706
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4708
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4709
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4711
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4712
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: chengming_3991_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4714
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4715
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4717
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4718
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4720
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-CHEN-211022/4721
Product: edge_gateway_3000_firmware					
Affected Version(s): * Up to (excluding) 1.9.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4723
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4724
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4726
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4727
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4729
Product: edge_gateway_5000_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4730
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4732
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4733
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4735
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4736
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-EDGE-211022/4737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: embedded_box_pc_3000_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4738
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4740
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4741
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4743
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4744
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: embedded_box_pc_5000_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4746
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4747
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4749
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4750
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4752
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-EMBE-211022/4753
Product: enterprise_sonic_distribution					
Affected Version(s): 4.0.0					
Use of Hard-coded Credentials	10-Oct-2022	7.5	Dell Enterprise SONiC OS, 4.0.0, 4.0.1, contain a cryptographic key vulnerability in SSH. An unauthenticated remote attacker could potentially exploit this	https://www.dell.com/support/kbdoc/en-us/000203395/dsa-2022-257-dell-emc-enterprise-sonic-security-update-for-ssh-cryptographic-	O-DEL-ENTE-211022/4754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, leading to unauthorized access to communication. **CVE ID : CVE-2022-34425**	key-vulnerability	
Affected Version(s): 4.0.1					
Use of Hard-coded Credentials	10-Oct-2022	7.5	Dell Enterprise SONiC OS, 4.0.0, 4.0.1, contain a cryptographic key vulnerability in SSH. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to unauthorized access to communication. **CVE ID : CVE-2022-34425**	https://www.dell.com/support/kbdoc/en-us/000203395/dsa-2022-257-dell-emc-enterprise-sonic-security-update-for-ssh-cryptographic-key-vulnerability	O-DEL-ENTE-211022/4755
Product: g3_15_3590_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4757
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4758
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4760
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4761
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4763
Product: g3_15_5590_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4764
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4766
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4767
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4769
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4770
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_1-211022/4771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: g3_3579_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4772
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4773
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4775
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4776
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4778
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4779
Product: g3_3779_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4781
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4782
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4784
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4785
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G3_3-211022/4787
Product: g5_5000_firmware					
Affected Version(s): * Up to (excluding) 1.10.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4788
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4790
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4791
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4793
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4794
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: g5_5090_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4796
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4798
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4799
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4801
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4802
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G5_5-211022/4803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: g7_17_7590_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4804
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4805
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4807
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4808
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4810
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4811
Product: g7_17_7790_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4813
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4814
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4816
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4817
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-G7_1-211022/4819
Product: inspiron_14_3467_firmware					
Affected Version(s): * Up to (excluding) 2.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4820
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4822
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4823
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4825
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4826
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_15_2-in-1_5582_firmware					
Affected Version(s): * Up to (excluding) 2.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4828
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4829
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4831
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4832
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4834
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4835
Product: inspiron_15_3567_firmware					
Affected Version(s): * Up to (excluding) 2.20.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4836
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4837
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4839
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4840
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4842
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4843
Product: inspiron_3277_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4845
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4846
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4848
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4849
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4851
Product: inspiron_3280_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4852
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4854
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4855
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4857
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4858
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3470_firmware					
Affected Version(s): * Up to (excluding) 2.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4860
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4861
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4863
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4864
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4866
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4867
Product: inspiron_3471_firmware					
Affected Version(s): * Up to (excluding) 1.11.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4869
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4870
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4872
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4873
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4875
Product: inspiron_3477_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4877
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4878
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4880
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4881
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4883
Product: inspiron_3480_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4884
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4886
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4887
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4889
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4890
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_3481_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4892
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4893
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4896
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4898
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4899
Product: inspiron_3482_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4901
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4902
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4904
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4905
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4907
Product: inspiron_3490_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4908
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4910
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4911
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4913
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4914
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3493_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4916
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4918
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4919
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4921
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4922
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: inspiron_3501_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4924
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4925
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4927
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4928
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4930
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4931
Product: inspiron_3502_firmware					
Affected Version(s): * Up to (excluding) 1.9.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4933
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4934
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4936
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4937
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4939
Product: inspiron_3580_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4940
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4942
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4943
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4945
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4946
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3581_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4948
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4949
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4951
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4952
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4954
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4955
Product: inspiron_3582_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4956
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4957
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4960
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4962
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4963
Product: inspiron_3590_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4965
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4966
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4968
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4969
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4971
Product: inspiron_3593_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4972
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4974
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4975
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4977
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4978
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3670_firmware					
Affected Version(s): * Up to (excluding) 2.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4980
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4981
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4983
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4984
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4986
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4987
Product: inspiron_3671_firmware					
Affected Version(s): * Up to (excluding) 1.11.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4989
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4990
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4992
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4993
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4995
Product: inspiron_3780_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4997
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4998
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/4999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5000
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5001
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5003
Product: inspiron_3781_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5004
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5006
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5007
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5009
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5010
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_3782_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5012
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5013
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5015
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5016
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5018
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5019
Product: inspiron_3790_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5021
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5022
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5024
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5025
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5027
Product: inspiron_3793_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5028
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5030
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5031
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5033
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5034
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_3880_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5036
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5038
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5039
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5041
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5042
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: inspiron_3881_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5044
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5045
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5047
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5048
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5050
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5051
Product: inspiron_5390_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5053
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5054
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5056
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5057
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5059
Product: inspiron_5391_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5060
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5062
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5063
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5065
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5066
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5400_firmware					
Affected Version(s): * Up to (excluding) 1.13.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5068
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5069
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5071
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5072
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5074
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5075
Product: inspiron_5401_firmware					
Affected Version(s): * Up to (excluding) 1.13.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5076
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5077
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5079
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5080
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5082
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5083
Product: inspiron_5477_firmware					
Affected Version(s): * Up to (excluding) 1.2.20					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5085
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5086
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5088
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5089
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5091
Product: inspiron_5480_firmware					
Affected Version(s): * Up to (excluding) 2.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5092
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5094
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5095
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5097
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5098
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5481_firmware					
Affected Version(s): * Up to (excluding) 2.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5100
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5101
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5103
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5104
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5106
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5107
Product: inspiron_5482_firmware					
Affected Version(s): * Up to (excluding) 2.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5109
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5110
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5112
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5113
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5115
Product: inspiron_5490_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5117
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5118
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5120
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5121
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5123
Product: inspiron_5491_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5124
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5126
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5127
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5129
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5130
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_5491_aio_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5132
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5133
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5135
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5136
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5138
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5139
Product: inspiron_5493_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5141
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5142
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5144
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5145
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5147
Product: inspiron_5494_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5148
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5150
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5151
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5153
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5154
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5498_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5156
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5158
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5159
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5161
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5162
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: inspiron_5570_firmware					
Affected Version(s): * Up to (excluding) 1.10.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5164
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5165
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5167
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5168
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5170
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5171
Product: inspiron_5580_firmware					
Affected Version(s): * Up to (excluding) 2.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5173
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5174
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5176
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5177
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5179
Product: inspiron_5583_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5180
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5182
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5183
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5185
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5186
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5584_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5188
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5189
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5191
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5192
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5194
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5195
Product: inspiron_5590_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5196
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5197
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5199
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5200
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5202
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5203
Product: inspiron_5591_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5205
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5206
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5208
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5209
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5211
Product: inspiron_5593_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5212
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5214
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5215
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5217
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5218
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_5594_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5220
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5221
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5223
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5224
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5226
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5227
Product: inspiron_5598_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5229
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5230
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5232
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5233
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5235
Product: inspiron_5680_firmware					
Affected Version(s): * Up to (excluding) 2.12.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5237
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5238
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5240
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5241
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5243
Product: inspiron_5770_firmware					
Affected Version(s): * Up to (excluding) 1.10.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5244
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5246
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5247
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5249
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5250
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_7000_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5252
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5253
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5256
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5258
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5259
Product: inspiron_7370_firmware					
Affected Version(s): * Up to (excluding) 1.25.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5261
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5262
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5264
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5265
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5267
Product: inspiron_7373_firmware					
Affected Version(s): * Up to (excluding) 1.25.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5268
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5270
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5271
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5273
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5274
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_7380_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5276
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5278
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5279
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5281
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5282
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: inspiron_7386_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5284
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5285
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5287
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5288
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5290
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5291
Product: inspiron_7390_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5293
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5294
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5296
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5297
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5299
Product: inspiron_7391_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5300
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5302
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5303
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5305
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5306
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_7490_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5308
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5309
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5311
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5312
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5314
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5315
Product: inspiron_7570_firmware					
Affected Version(s): * Up to (excluding) 1.25.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5316
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5317
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5319
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5320
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5322
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5323
Product: inspiron_7573_firmware					
Affected Version(s): * Up to (excluding) 1.25.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5325
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5326
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5328
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5329
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5331
Product: inspiron_7580_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5332
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5334
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5335
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5337
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5338
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_7586_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5340
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5341
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5343
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5344
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5346
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5347
Product: inspiron_7590_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5349
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5350
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5352
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5353
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5355
Product: inspiron_7591_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5357
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5358
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5360
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5361
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5363
Product: inspiron_7700_aio_firmware					
Affected Version(s): * Up to (excluding) 1.13.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5364
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5366
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5367
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5369
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5370
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: inspiron_7777_firmware					
Affected Version(s): * Up to (excluding) 1.2.20					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5372
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5373
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5375
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5376
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5378
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5379
Product: inspiron_7786_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5381
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5382
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5384
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5385
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5387
Product: inspiron_7790_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5388
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5390
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5391
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5393
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5394
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: inspiron_7791_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5396
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5398
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5399
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5401
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5402
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-INSP-211022/5403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_3120_firmware					
Affected Version(s): * Up to (excluding) 1.10.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5404
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5405
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5407
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5408
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5410
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5411
Product: latitude_3180_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5413
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5414
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5416
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5417
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5419
Product: latitude_3189_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5420
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5422
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5423
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5425
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5426
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_3190_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5428
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5429
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5431
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5432
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5434
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5435
Product: latitude_3190_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5436
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5437
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5439
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5440
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5442
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5443
Product: latitude_3300_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5445
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5446
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5448
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5449
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5451
Product: latitude_3301_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5452
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5454
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5455
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5457
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5458
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_3310_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5460
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5461
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5463
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5464
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5466
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5467
Product: latitude_3310_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5469
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5470
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5472
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5473
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5475
Product: latitude_3379_firmware					
Affected Version(s): * Up to (excluding) 1.0.36					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5477
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5478
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5480
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5481
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5483
Product: latitude_3390_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5484
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5486
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5487
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5489
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5490
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: latitude_3480_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5492
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5493
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5495
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5496
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5498
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5499
Product: latitude_3490_firmware					
Affected Version(s): * Up to (excluding) 1.25.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5501
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5502
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5504
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5505
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5507
Product: latitude_3580_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5508
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5510
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5511
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5513
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5514
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_3590_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5516
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5518
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5521
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5522
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_5280_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5524
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5525
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5528
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5530
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5531
Product: latitude_5285_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5533
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5534
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5536
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5537
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5539
Product: latitude_5289_firmware					
Affected Version(s): * Up to (excluding) 1.29.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5540
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5542
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5543
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5545
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5546
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5290_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5548
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5549
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5551
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5552
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5554
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5555
Product: latitude_5290_firmware					
Affected Version(s): * Up to (excluding) 1.24.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5556
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5557
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5559
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5560
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5562
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5563
Product: latitude_5300_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5565
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5566
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5568
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5569
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5571
Product: latitude_5300_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5572
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5574
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5575
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5577
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5578
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5310_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5580
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5581
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5583
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5584
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5586
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5587
Product: latitude_5310_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5589
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5590
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5592
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5593
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5595
Product: latitude_5400_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5597
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5598
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5600
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5601
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5603
Product: latitude_5401_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5604
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5606
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5609
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5610
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: latitude_5410_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5612
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5613
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5615
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5616
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5618
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5619
Product: latitude_5411_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5621
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5622
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5624
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5625
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5627
Product: latitude_5414_rugged_firmware					
Affected Version(s): * Up to (excluding) 1.36.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5628
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5630
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5631
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5633
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5634
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5420_rugged_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5636
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5638
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5639
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5641
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5642
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_5480_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5644
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5645
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5647
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5648
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5650
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5651
Product: latitude_5488_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5653
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5654
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5656
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5657
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5659
Product: latitude_5490_firmware					
Affected Version(s): * Up to (excluding) 1.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5660
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5662
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5663
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5665
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5666
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5491_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5668
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5669
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5671
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5672
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5674
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5675
Product: latitude_5495_firmware					
Affected Version(s): * Up to (excluding) 1.9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5676
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5677
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5679
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5680
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5682
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5683
Product: latitude_5500_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5685
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5686
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5688
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5689
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5691
Product: latitude_5501_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5692
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5694
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5695
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5697
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5698
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_5510_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5700
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5701
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5703
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5704
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5706
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5707
Product: latitude_5511_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5709
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5710
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5712
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5713
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5715
Product: latitude_5580_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5717
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5718
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5720
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5721
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5723
Product: latitude_5590_firmware					
Affected Version(s): * Up to (excluding) 1.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5724
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5726
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5727
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5729
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5730
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: latitude_5591_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5732
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5733
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5735
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5736
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5738
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5739
Product: latitude_7200_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5741
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5742
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5744
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5745
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5747
Product: latitude_7210_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5748
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5750
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5751
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5753
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5754
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7212_rugged_extreme_tablet_firmware					
Affected Version(s): * Up to (excluding) 1.40.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5756
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5758
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5759
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5761
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5762
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_7214_rugged_extreme_firmware					
Affected Version(s): * Up to (excluding) 1.36.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5764
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5765
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5767
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5768
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5770
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5771
Product: latitude_7220ex_rugged_extreme_tablet_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5773
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5774
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5776
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5777
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5779
Product: latitude_7220_rugged_extreme_tablet_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5780
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5782
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5783
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5785
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5786
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7275_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5788
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5789
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5791
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5792
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5794
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5795
Product: latitude_7290_firmware					
Affected Version(s): * Up to (excluding) 1.27.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5796
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5797
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5799
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5800
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5802
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5803
Product: latitude_7300_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5805
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5806
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5808
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5809
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5811
Product: latitude_7310_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5812
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5814
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5815
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5817
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5818
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7370_firmware					
Affected Version(s): * Up to (excluding) 1.30.3					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5820
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5821
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5823
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5824
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5826
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5827
Product: latitude_7380_firmware					
Affected Version(s): * Up to (excluding) 1.27.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5829
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5830
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5832
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5833
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5835
Product: latitude_7389_firmware					
Affected Version(s): * Up to (excluding) 1.29.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5837
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5838
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5840
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5841
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5843
Product: latitude_7390_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5844
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5846
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5847
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5849
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5850
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: latitude_7390_firmware					
Affected Version(s): * Up to (excluding) 1.27.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5852
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5853
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5855
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5856
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5858
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5859
Product: latitude_7400_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5861
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5862
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5864
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5865
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5867
Product: latitude_7400_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5868
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5870
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5871
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5873
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5874
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7410_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5876
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5878
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5879
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5881
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5882
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: latitude_7414_rugged_extreme_firmware					
Affected Version(s): * Up to (excluding) 1.36.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5884
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5885
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5887
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5888
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5890
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5891
Product: latitude_7424_rugged_extreme_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5893
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5894
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5896
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5897
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5899
Product: latitude_7480_firmware					
Affected Version(s): * Up to (excluding) 1.27.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5900
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5902
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5903
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5905
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5906
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_7490_firmware					
Affected Version(s): * Up to (excluding) 1.27.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5908
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5909
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5911
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5912
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5914
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5915
Product: latitude_9410_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5916
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5917
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5919
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5920
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5922
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5923
Product: latitude_9510_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5925
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5926
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5928
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5929
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5931
Product: latitude_e5270_firmware					
Affected Version(s): * Up to (excluding) 1.32.3					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5932
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5934
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5935
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5937
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5938
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: latitude_e5470_firmware					
Affected Version(s): * Up to (excluding) 1.32.3					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5940
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5941
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5943
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5944
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5946
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5947
Product: latitude_e5570_firmware					
Affected Version(s): * Up to (excluding) 1.32.3					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5949
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5950
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5952
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5953
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5955
Product: latitude_e7270_firmware					
Affected Version(s): * Up to (excluding) 1.35.3					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5957
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5958
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5960
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5961
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5963
Product: latitude_e7470_firmware					
Affected Version(s): * Up to (excluding) 1.35.3					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5964
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5966
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5967
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5969
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5970
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-LATI-211022/5971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: optiplex_3040_firmware					
Affected Version(s): * Up to (excluding) 1.20.1					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5972
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5973
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5975
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5976
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5978
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5979
Product: optiplex_3046_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5981
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5982
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5984
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5985
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5987
Product: optiplex_3050_aio_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5988
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5990
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5991
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5993
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5994
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_3050_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5996
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5998
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/5999
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6001
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6002
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: optiplex_3060_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6004
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6005
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6007
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6008
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6010
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6011
Product: optiplex_3070_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6013
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6014
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6016
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6017
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6019
Product: optiplex_3080_firmware					
Affected Version(s): * Up to (excluding) 2.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6020
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6022
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6023
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6025
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6026
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_3090_firmware					
Affected Version(s): * Up to (excluding) 2.7.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6028
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6029
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6031
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6032
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6034
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6035
Product: optiplex_3280_aio_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6036
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6037
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6039
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6040
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6042
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6043
Product: optiplex_5050_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6045
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6046
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6048
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6049
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6051
Product: optiplex_5055_firmware					
Affected Version(s): * Up to (excluding) 1.7.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6052
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6054
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6055
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6057
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6058
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_5060_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6060
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6061
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6063
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6064
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6066
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6067
Product: optiplex_5070_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6069
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6070
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6072
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6073
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6075
Product: optiplex_5080_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6077
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6078
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6080
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6081
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6083
Product: optiplex_5260_all-in-one_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6084
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6086
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6087
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6089
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6090
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: optiplex_5480_all-in-one_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6092
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6093
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6095
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6096
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6098
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6099
Product: optiplex_7040_firmware					
Affected Version(s): * Up to (excluding) 1.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6101
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6102
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6104
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6105
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6107
Product: optiplex_7050_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6108
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6110
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6111
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6113
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6114
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_7060_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6116
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6118
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6119
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6121
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6122
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: optiplex_7070_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6124
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6125
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6127
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6128
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6130
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6131
Product: optiplex_7070_ultra_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6133
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6134
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6136
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6137
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6139
Product: optiplex_7071_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6140
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6142
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6143
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6145
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6146
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_7080_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6148
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6149
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6151
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6152
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6154
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6155
Product: optiplex_7450_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6156
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6157
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6159
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6160
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6162
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6163
Product: optiplex_7460_all_in_one_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6165
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6166
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6168
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6169
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6171
Product: optiplex_7470_all-in-one_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6172
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6174
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6175
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6177
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6178
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: optiplex_7480_all-in-one_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6180
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6181
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6183
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6184
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6186
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6187
Product: optiplex_xe3_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6189
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6190
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6192
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6193
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-OPTI-211022/6195
Product: precision_3240_compact_firmware					
Affected Version(s): * Up to (excluding) 1.13.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6197
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6198
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6200
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6201
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6203
Product: precision_3420_tower_firmware					
Affected Version(s): * Up to (excluding) 2.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6204
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6206
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6207
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6209
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6210
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: precision_3430_tower_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6212
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6213
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6215
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6216
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6218
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6219
Product: precision_3431_tower_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6221
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6222
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6224
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6225
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6227
Product: precision_3440_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6228
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6230
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6231
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6233
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6234
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_3510_firmware					
Affected Version(s): * Up to (excluding) 1.32.3					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6236
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6238
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6239
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6241
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6242
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: precision_3520_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6244
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6245
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6247
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6248
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6250
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6251
Product: precision_3540_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6253
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6254
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6256
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6257
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6259
Product: precision_3541_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6260
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6262
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6263
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6265
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6266
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_3550_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6268
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6269
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6271
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6272
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6274
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6275
Product: precision_3551_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6276
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6277
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6279
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6280
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6282
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6283
Product: precision_3620_tower_firmware					
Affected Version(s): * Up to (excluding) 2.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6285
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6286
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6288
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6289
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6291
Product: precision_3630_tower_firmware					
Affected Version(s): * Up to (excluding) 2.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6292
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6294
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6295
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6297
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6298
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_3640_tower_firmware					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6300
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6301
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6303
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6304
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6306
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6307
Product: precision_3930_rack_firmware					
Affected Version(s): * Up to (excluding) 2.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6309
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6310
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6312
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6313
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6315
Product: precision_5510_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6317
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6318
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6320
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6321
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6323
Product: precision_5530_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.20.8					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6324
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6326
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6327
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6329
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6330
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: precision_5530_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6332
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6333
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6335
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6336
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6338
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6339
Product: precision_5540_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6341
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6342
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6344
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6345
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6347
Product: precision_5720_aio_firmware					
Affected Version(s): * Up to (excluding) 2.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6348
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6350
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6351
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6353
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6354
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_5820_tower_firmware					
Affected Version(s): * Up to (excluding) 2.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6356
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6358
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6359
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6361
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6362
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: precision_7510_firmware					
Affected Version(s): * Up to (excluding) 1.28.3					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6364
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6365
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6367
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6368
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6370
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6371
Product: precision_7520_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6373
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6374
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6376
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6377
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6379
Product: precision_7530_firmware					
Affected Version(s): * Up to (excluding) 1.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6380
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6382
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6383
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6385
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6386
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_7540_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6388
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6389
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6391
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6392
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6394
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6395
Product: precision_7550_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6396
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6397
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6399
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6400
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6402
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6403
Product: precision_7710_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6405
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6406
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6408
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6409
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6411
Product: precision_7720_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6412
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6414
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6415
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6417
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6418
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: precision_7730_firmware					
Affected Version(s): * Up to (excluding) 1.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6420
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6421
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6424
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6426
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6427
Product: precision_7740_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6429
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6430
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6432
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6433
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6435
Product: precision_7750_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6437
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6438
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6440
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6441
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6443
Product: precision_7820_tower_firmware					
Affected Version(s): * Up to (excluding) 2.26.1					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6444
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6446
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6447
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6449
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6450
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: precision_7920_tower_firmware					
Affected Version(s): * Up to (excluding) 2.26.1					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6452
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6453
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6455
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6456
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6458
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-PREC-211022/6459
Product: vostro_3070_firmware					
Affected Version(s): * Up to (excluding) 2.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6461
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6462
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6464
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6465
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6467
Product: vostro_3267_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6468
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6470
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6471
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6473
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6474
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_3268_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6476
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6478
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6479
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6481
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6482
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: vostro_3401_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6484
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6485
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6487
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6488
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6490
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6491
Product: vostro_3470_firmware					
Affected Version(s): * Up to (excluding) 2.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6493
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6494
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6496
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6497
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6499
Product: vostro_3471_firmware					
Affected Version(s): * Up to (excluding) 1.11.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6500
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6502
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6503
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6505
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6506
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_3480_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6508
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6509
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6511
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6512
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6514
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6515
Product: vostro_3481_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6516
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6517
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6520
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6522
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6523
Product: vostro_3490_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6525
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6526
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6528
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6529
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6531
Product: vostro_3501_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6532
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6534
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6535
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6537
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6538
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_3580_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6540
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6541
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6544
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6546
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6547
Product: vostro_3581_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6549
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6550
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6552
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6553
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6555
Product: vostro_3582_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6557
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6558
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6560
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6561
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6563
Product: vostro_3583_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6564
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6566
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6567
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6569
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6570
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: vostro_3584_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6572
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6573
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6575
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6576
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6578
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6579
Product: vostro_3590_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6581
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6582
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6584
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6585
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6587
Product: vostro_3667_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6588
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6590
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6591
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6593
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6594
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_3668_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6596
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6598
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6599
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6601
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6602
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: vostro_3669_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6604
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6605
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6608
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6610
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6611
Product: vostro_3670_firmware					
Affected Version(s): * Up to (excluding) 2.24.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6613
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6614
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6616
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6617
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6619
Product: vostro_3671_firmware					
Affected Version(s): * Up to (excluding) 1.11.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6620
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6622
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6623
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6625
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6626
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_3681_firmware					
Affected Version(s): * Up to (excluding) 2.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6628
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6629
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6631
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6632
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6634
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6635
Product: vostro_3881_firmware					
Affected Version(s): * Up to (excluding) 2.14.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6636
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6637
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6639
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6640
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6642
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6643
Product: vostro_3888_firmware					
Affected Version(s): * Up to (excluding) 2.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6645
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6646
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6648
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6649
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6651
Product: vostro_5090_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6652
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6654
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6655
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6657
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6658
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: vostro_5390_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6660
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6661
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6663
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6664
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6666
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6667
Product: vostro_5391_firmware					
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6669
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6670
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6672
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6673
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6675
Product: vostro_5581_firmware					
Affected Version(s): * Up to (excluding) 2.16.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6677
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6678
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6680
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6681
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6683
Product: vostro_5590_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6684
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6686
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6687
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6689
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6690
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: vostro_5591_firmware					
Affected Version(s): * Up to (excluding) 1.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6692
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6693
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6695
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6696
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6698
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6699
Product: vostro_5880_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6701
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6702
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6704
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6705
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6707
Product: vostro_7590_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6708
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6710
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6711
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6713
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6714
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-VOST-211022/6715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: wyse_5070_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6716
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6718
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6719
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6721
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6722
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wyse_5470_all-in-one_firmware					
Affected Version(s): * Up to (excluding) 1.16.1					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6724
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6725
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6727
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6728
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6730
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6731
Product: wyse_5470_firmware					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6733
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6734
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6736
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6737
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6739
Product: wyse_7040_thin_client_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6740
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6742
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6743
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6745
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6746
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-WYSE-211022/6747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: wyse_thinos					
Affected Version(s): * Up to (excluding) 9.3.2102					
Incorrect Comparison	10-Oct-2022	4.9	Dell Wyse ThinOS 2205 contains a Regular Expression Denial of Service Vulnerability in UI. An admin privilege attacker could potentially exploit this vulnerability, leading to denial-of-service. **CVE ID : CVE-2022-34402**	https://www.dell.com/support/kbdoc/en-us/000203376/dsa-2022-247-dell-wyse-thinos-security-update-for-a-regular-expression-vulnerability	O-DEL-WYSE-211022/6748
Product: xps_13_7390_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6750
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6751
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6753
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6754
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6756
Product: xps_13_7390_firmware					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6757
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32487		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6759
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6760
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32491		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6762
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6763
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32484		
Product: xps_13_9300_firmware					
Affected Version(s): * Up to (excluding) 1.14.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6765
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6766
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6768
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6769
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6771
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6772
Product: xps_13_9365_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 2.23.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6774
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6775
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6777
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6778
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6780
Product: xps_13_9370_firmware					
Affected Version(s): * Up to (excluding) 1.21.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6781
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6783
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6784
Buffer Copy without Checking	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6786
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6787
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: xps_13_9380_firmware					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6789
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6791
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6792
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6794
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6795
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: xps_15_7590_firmware					
Affected Version(s): * Up to (excluding) 1.26.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6797
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6798
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32488		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6800
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6801
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32493		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6803
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6804
Product: xps_15_9575_2-in-1_firmware					
Affected Version(s): * Up to (excluding) 1.22.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32485**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6806
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6807
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in SMRAM. **CVE ID : CVE-2022-32489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6809
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6810
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to modify a UEFI variable. **CVE ID : CVE-2022-32483**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6812
Product: xps_7590_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6813
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6815
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6816
Buffer Copy without Checking Size of Input ('Classic	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**		
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6818
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6819
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**		
Product: xps_8930_firmware					
Affected Version(s): * Up to (excluding) 1.1.24					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6821
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6822
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6824
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6825
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6827
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6828
Product: xps_8940_firmware					
Affected Version(s): * Up to (excluding) 2.9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32485**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6829
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6830
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32489**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6832
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6833
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32483**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6835
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6836
Product: xps_8950_firmware					
Affected Version(s): * Up to (excluding) 1.5.0					
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32485		
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32487**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6838
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32488**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6839
Improper Input Validation	12-Oct-2022	7.8	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM.	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32489		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Oct-2022	7.8	Dell Client BIOS contains a Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause an arbitrary write during SMM. **CVE ID : CVE-2022-32491**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6841
Out-of-bounds Write	12-Oct-2022	7.8	Dell BIOS contains an Stack-Based Buffer Overflow vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution in SMRAM. **CVE ID : CVE-2022-32493**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6842
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32483		
Improper Input Validation	12-Oct-2022	4.4	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability in order to modify a UEFI variable. **CVE ID : CVE-2022-32484**	https://www.dell.com/support/kbdoc/000203758	O-DEL-XPS_-211022/6844
Vendor: foresightsports					
Product: gc3_launch_monitor_firmware					
Affected Version(s): * Up to (excluding) 1.5.0.2					
Incorrect Default Permissions	13-Oct-2022	8	Foresight GC3 Launch Monitor 1.3.15.68 ships with a Target Communication Framework (TCF) service enabled. This service listens on a TCP port on all interfaces and allows for process debugging, file system modification, and terminal access as the root user. In conjunction with a hosted wireless access point and the known passphrase of FSSPORTS, an attacker could use	N/A	O-FOR-GC3_-211022/6845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this service to modify a device and steal intellectual property. **CVE ID : CVE-2022-40187**		
Vendor: generex					
Product: cs141_firmware					
Affected Version(s): * Up to (excluding) 2.08					
N/A	06-Oct-2022	7.2	Generex CS141 through 2.10 allows remote command execution by administrators via a web interface that reaches run_update in /usr/bin/gxserve-update.sh (e.g., command execution can occur via a reverse shell installed by install.sh). **CVE ID : CVE-2022-42457**	https://www.generex.de/support/downloads/ups/cs141, https://www.generex.de/products/ups/	O-GEN-CS14-211022/6846
Vendor: Google					
Product: android					
Affected Version(s): -					
Out-of-bounds Write	14-Oct-2022	7.8	In SitRilClient_OnResponse of SitRilSe.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution	https://source.android.com/security/bulletin/pixel/2022-10-01	O-GOO-ANDR-211022/6847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-223086933References: N/A **CVE ID : CVE-2022-20397**		
Use After Free	11-Oct-2022	7.8	In binder_inc_ref_for_node of binder.c, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239630375References: Upstream kernel **CVE ID : CVE-2022-20421**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6848
Missing Authorization	11-Oct-2022	7.8	There is an missing authorization issue in the system service. Since the component does not have	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission check , resulting in Local Elevation of privilege.Product: AndroidVersions: Android SoCAndroid ID: A-242221233 **CVE ID : CVE-2022-20430**		
Missing Authorization	11-Oct-2022	7.8	There is an missing authorization issue in the system service. Since the component does not have permission check , resulting in Local Elevation of privilege.Product: AndroidVersions: Android SoCAndroid ID: A-242221238 **CVE ID : CVE-2022-20431**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6850
Missing Authorization	11-Oct-2022	7.8	There is an missing authorization issue in the system service. Since the component does not have permission check and permission protection,, resulting in Local Elevation of privilege.Product: AndroidVersions: Android SoCAndroid ID: A-242221899	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20432		
Missing Authorization	11-Oct-2022	7.8	There is an missing authorization issue in the system service. Since the component does not have permission check , resulting in Local Elevation of privilege.Product: AndroidVersions: Android SoCAndroid ID: A-242221901 **CVE ID : CVE-2022-20433**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6852
Missing Authorization	11-Oct-2022	7.8	There is an missing authorization issue in the system service. Since the component does not have permission check , resulting in Local Elevation of privilege.Product: AndroidVersions: Android SoCAndroid ID: A-242244028 **CVE ID : CVE-2022-20434**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6853
Incorrect Default Permissions	11-Oct-2022	7.8	There is a Unauthorized service in the system service, may cause the system reboot. Since the component does not have	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission check and permission protection, resulting in EoP problem.Product: AndroidVersions: Android SoCAndroid ID: A-242248367 **CVE ID : CVE-2022-20435**		
Incorrect Default Permissions	11-Oct-2022	7.8	There is an unauthorized service in the system service. Since the component does not have permission check, resulting in Local Elevation of privilege.Product: AndroidVersions: Android SoCAndroid ID: A-242248369 **CVE ID : CVE-2022-20436**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6855
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	In emulation_proc_handler of armv8_deprecated.c, there is a possible way to corrupt memory due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-237540956References: Upstream kernel **CVE ID : CVE-2022-20422**		
Use After Free	11-Oct-2022	6.7	In io_identity_cow of io_uring.c, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238177383References: Upstream kernel **CVE ID : CVE-2022-20409**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6857
Improper Synchronization	07-Oct-2022	6.7	In isp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07262305; Issue ID: ALPS07262305. **CVE ID : CVE-2022-26452**		
N/A	11-Oct-2022	5.5	In Messaging, There has unauthorized broadcast, this could cause Local Deny of Service.Product: AndroidVersions: Android SoCAndroid ID: A-242258929 **CVE ID : CVE-2022-20437**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6859
N/A	11-Oct-2022	5.5	In Messaging, There has unauthorized broadcast, this could cause Local Deny of Service.Product: AndroidVersions: Android SoCAndroid ID: A-242259920 **CVE ID : CVE-2022-20438**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6860
N/A	11-Oct-2022	5.5	In Messaging, There has unauthorized provider, this could cause Local Deny of Service.Product: AndroidVersions: Android SoCAndroid ID: A-242266172	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20439		
N/A	11-Oct-2022	5.5	In Messaging, There has unauthorized broadcast, this could cause Local Deny of Service.Product: AndroidVersions: Android SoCAndroid ID: A-242259918 **CVE ID : CVE-2022-20440**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6862
N/A	14-Oct-2022	5.5	In various functions of ap_input_processor.c, there is a possible way to record audio during a phone call due to a logic error in the code. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-236042696References: N/A **CVE ID : CVE-2022-20464**	https://source.android.com/security/bulletin/pixel/2022-10-01	O-GOO-ANDR-211022/6863
Integer Overflow or	11-Oct-2022	4.6	In rndis_set_response of rndis.c, there is a possible out of	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			bounds write due to an integer overflow. This could lead to local escalation of privilege if a malicious USB device is attached with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239842288References: Upstream kernel **CVE ID : CVE-2022-20423**		
Affected Version(s): 10.0					
N/A	11-Oct-2022	8.8	In CarSettings of app packages, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11	https://source.android.com/security/bulletin/aaos/2022-10-01	O-GOO-ANDR-211022/6865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12 Android-12LAndroid ID: A-220741473 **CVE ID : CVE-2022-20429**		
N/A	11-Oct-2022	7.8	In handleFullScreenIntent of StatusBarNotificationActivityStarter.java, there is a possible bypass of the restriction of starting activity from background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-231322873 **CVE ID : CVE-2022-20415**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6866
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Out-of-bounds Write	07-Oct-2022	7.8	A heap-based overflow vulnerability in makeContactAGIF in libagifencoder.quram.so library prior to SMR Oct-2022 Release 1 allows attacker to perform code execution. **CVE ID : CVE-2022-39852**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6868
Use After Free	07-Oct-2022	7.8	A use after free vulnerability in perf-mgr driver prior to SMR Oct-2022 Release 1 allows attacker to cause memory access fault. **CVE ID : CVE-2022-39853**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6869
N/A	07-Oct-2022	7.8	Improper protection in IOMMU prior to SMR Oct-2022 Release 1 allows unauthorized	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to secure memory. **CVE ID : CVE-2022-39854**		
Out-of-bounds Read	11-Oct-2022	7.5	In avrc_ctrl_pars_vendor_rsp of avrc_pars_ct.cc, there is a possible out of bounds read due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-205570663 **CVE ID : CVE-2022-20410**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6871
Out-of-bounds Read	11-Oct-2022	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230794395 **CVE ID : CVE-2022-20412**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Oct-2022	5.5	In queryInternal of CallLogProvider.java, there is a possible access to voicemail information due to SQL injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-224771921 **CVE ID : CVE-2022-20351**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6873
N/A	11-Oct-2022	5.5	In start of Threads.cpp, there is a possible way to record audio during a phone call due to a logic error in the code. This could lead to local	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235850634 **CVE ID : CVE-2022-20413**		
Uncontrolled Resource Consumption	11-Oct-2022	5.5	In addAutomaticZenRule of ZenModeHelper.java, there is a possible permanent degradation of performance due to resource exhaustion. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235823407 **CVE ID : CVE-2022-20425**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-Oct-2022	5.3	Use after free vulnerability in set_nft_pid and signal_handler function of NFC driver prior to SMR Oct-2022 Release 1 allows attackers to perform malicious actions. **CVE ID : CVE-2022-39847**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6876
N/A	11-Oct-2022	5	In getInputMethodWindowVisibleHeight of InputMethodManagerService.java, there is a possible way to determine when another app is showing an IME due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-204906124 **CVE ID : CVE-2022-20394**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Oct-2022	4.3	Improper access control vulnerability in FACM application prior to SMR Oct-2022 Release 1 allows a local attacker to connect arbitrary AP and Bluetooth devices. **CVE ID : CVE-2022-39855**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6878
Exposure of Sensitive Information to an Unauthorized Actor	07-Oct-2022	3.3	Exposure of sensitive information in AT_Distributor prior to SMR Oct-2022 Release 1 allows local attacker to access SerialNo via log. **CVE ID : CVE-2022-39848**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6879
N/A	07-Oct-2022	3.3	Improper access control in knox_vpn_policy service prior to SMR Oct-2022 Release 1 allows allows unauthorized read of configuration data. **CVE ID : CVE-2022-39849**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6880
N/A	07-Oct-2022	3.3	Improper access control in mum_container_policy service prior to SMR Oct-2022 Release 1 allows allows	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read of configuration data. **CVE ID : CVE-2022-39850**		
N/A	07-Oct-2022	3.3	Improper access control vulnerability in CocktailBarService prior to SMR Oct-2022 Release 1 allows local attacker to bind service that require BIND_REMOTEVIEWS permission. **CVE ID : CVE-2022-39851**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6882
Affected Version(s): 11.0					
Incorrect Authorization	07-Oct-2022	9.8	Improper authorization in Dynamic Lockscreen prior to SMR Sep-2022 Release 1 in Android R(11) and 3.3.03.66 in Android S(12) allows unauthorized use of javascript interface api. **CVE ID : CVE-2022-39862**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	O-GOO-ANDR-211022/6883
N/A	11-Oct-2022	8.8	In CarSettings of app packages, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of	https://source.android.com/security/bulletin/aaos/2022-10-01	O-GOO-ANDR-211022/6884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-220741473 **CVE ID : CVE-2022-20429**		
N/A	11-Oct-2022	7.8	In handleFullScreenIntent of StatusBarNotificationActivityStarter.java, there is a possible bypass of the restriction of starting activity from background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-231322873 **CVE ID : CVE-2022-20415**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095; Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6886
Out-of-bounds Write	07-Oct-2022	7.8	A heap-based overflow vulnerability in makeContactAGIF in libagifencoder.quram.so library prior to SMR Oct-2022 Release 1 allows attacker to perform code execution. **CVE ID : CVE-2022-39852**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6887
Use After Free	07-Oct-2022	7.8	A use after free vulnerability in perf-mgr driver prior to SMR Oct-2022 Release 1 allows attacker to	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause memory access fault. **CVE ID : CVE-2022-39853**		
N/A	07-Oct-2022	7.8	Improper protection in IOMMU prior to SMR Oct-2022 Release 1 allows unauthorized access to secure memory. **CVE ID : CVE-2022-39854**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6889
Out-of-bounds Read	11-Oct-2022	7.5	In avrc_ctrl_pars_vendor_rsp of avrc_pars_ct.cc, there is a possible out of bounds read due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-205570663 **CVE ID : CVE-2022-20410**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6890
Improper Resource	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible	https://corp.mediatek.com/pr	O-GOO-ANDR-211022/6891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	oduct-security-bulletin/October-2022	
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6892
Out-of-bounds Read	11-Oct-2022	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230794395 **CVE ID : CVE-2022-20412**		
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6894
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**		
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6896
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Oct-2022	5.5	In queryInternal of CallLogProvider.java, there is a possible access to voicemail information due to SQL injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12LAndroid ID: A-224771921 **CVE ID : CVE-2022-20351**		
N/A	11-Oct-2022	5.5	In start of Threads.cpp, there is a possible way to record audio during a phone call due to a logic error in the code. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235850634 **CVE ID : CVE-2022-20413**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6898
Uncontrolled Resource Consumption	11-Oct-2022	5.5	In addAutomaticZenRule of ZenModeHelper.java, there is a possible permanent degradation of performance due to resource exhaustion. This could lead to local	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235823407 **CVE ID : CVE-2022-20425**		
Use After Free	07-Oct-2022	5.3	Use after free vulnerability in set_nft_pid and signal_handler function of NFC driver prior to SMR Oct-2022 Release 1 allows attackers to perform malicious actions. **CVE ID : CVE-2022-39847**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6900
Improper Privilege Management	07-Oct-2022	5.3	Improper access control vulnerability in ProfileSharingAccount in Group Sharing prior to versions 13.0.6.15 in Android S(12), 13.0.6.14 in Android R(11) and below allows attackers to identify the device. **CVE ID : CVE-2022-39877**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	O-GOO-ANDR-211022/6901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	5	In getInputMethodWindowVisibleHeight of InputMethodManagerService.java, there is a possible way to determine when another app is showing an IME due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-204906124 **CVE ID : CVE-2022-20394**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6902
N/A	07-Oct-2022	4.3	Improper access control vulnerability in FACM application prior to SMR Oct-2022 Release 1 allows a local attacker to connect arbitrary AP and Bluetooth devices. **CVE ID : CVE-2022-39855**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Oct-2022	3.3	Improper restriction of broadcasting Intent in MouseNKeyHidDevice prior to SMR Oct-2022 Release 1 leaks MAC address of the connected Bluetooth device. **CVE ID : CVE-2022-36868**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6904
Exposure of Sensitive Information to an Unauthorized Actor	07-Oct-2022	3.3	Exposure of sensitive information in AT_Distributor prior to SMR Oct-2022 Release 1 allows local attacker to access SerialNo via log. **CVE ID : CVE-2022-39848**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6905
N/A	07-Oct-2022	3.3	Improper access control in knox_vpn_policy service prior to SMR Oct-2022 Release 1 allows allows unauthorized read of configuration data. **CVE ID : CVE-2022-39849**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6906
N/A	07-Oct-2022	3.3	Improper access control in mum_container_policy service prior to SMR Oct-2022 Release 1 allows allows	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read of configuration data. **CVE ID : CVE-2022-39850**		
N/A	07-Oct-2022	3.3	Improper access control vulnerability in CocktailBarService prior to SMR Oct-2022 Release 1 allows local attacker to bind service that require BIND_REMOTEVIEWS permission. **CVE ID : CVE-2022-39851**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6908
Affected Version(s): 12.0					
Incorrect Authorization	07-Oct-2022	9.8	Improper authorization in Dynamic Lockscreen prior to SMR Sep-2022 Release 1 in Android R(11) and 3.3.03.66 in Android S(12) allows unauthorized use of javascript interface api. **CVE ID : CVE-2022-39862**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	O-GOO-ANDR-211022/6909
N/A	11-Oct-2022	8.8	In CarSettings of app packages, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of	https://source.android.com/security/bulletin/aaos/2022-10-01	O-GOO-ANDR-211022/6910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-220741473 **CVE ID : CVE-2022-20429**		
N/A	11-Oct-2022	7.8	In handleFullScreenIntent of StatusBarNotificationActivityStarter.java, there is a possible bypass of the restriction of starting activity from background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-231322873 **CVE ID : CVE-2022-20415**		
Out-of-bounds Write	11-Oct-2022	7.8	In audioTransportsToHal of HidlUtils.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237717857 **CVE ID : CVE-2022-20416**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6912
Out-of-bounds Write	11-Oct-2022	7.8	In audioTransportsToHal of HidlUtils.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Produc	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			t: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237288416 **CVE ID : CVE-2022-20417**		
Deserialization of Untrusted Data	07-Oct-2022	7.8	In telephony, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319121; Issue ID: ALPS07319121. **CVE ID : CVE-2022-26471**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6914
Deserialization of Untrusted Data	07-Oct-2022	7.8	In ims, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319095;	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07319095. **CVE ID : CVE-2022-26472**		
Out-of-bounds Write	07-Oct-2022	7.8	A heap-based overflow vulnerability in makeContactAGIF in libagifencoder.quram.so library prior to SMR Oct-2022 Release 1 allows attacker to perform code execution. **CVE ID : CVE-2022-39852**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6916
Use After Free	07-Oct-2022	7.8	A use after free vulnerability in perf-mgr driver prior to SMR Oct-2022 Release 1 allows attacker to cause memory access fault. **CVE ID : CVE-2022-39853**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6917
N/A	07-Oct-2022	7.8	Improper protection in IOMMU prior to SMR Oct-2022 Release 1 allows unauthorized access to secure memory. **CVE ID : CVE-2022-39854**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6918
Improper Input Validation	07-Oct-2022	7.5	In ril, there is a possible system crash due to an incorrect bounds	https://corp.mediatek.com/product-security-	O-GOO-ANDR-211022/6919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07257259; Issue ID: ALPS07257259. **CVE ID : CVE-2022-32591**	bulletin/October-2022	
Out-of-bounds Read	11-Oct-2022	7.5	In avrc_ctrl_pars_vendor_rsp of avrc_pars_ct.cc, there is a possible out of bounds read due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-205570663 **CVE ID : CVE-2022-20410**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	11-Oct-2022	7.5	In pickStartSeq of AAVCAssembler.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-231986464 **CVE ID : CVE-2022-20418**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6921
Improper Resource Shutdown or Release	07-Oct-2022	7.5	In Wi-Fi driver, there is a possible way to disconnect Wi-Fi due to an improper resource release. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07030600; Issue ID: ALPS07030600. **CVE ID : CVE-2022-32589**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-Oct-2022	6.7	In wlan, there is a possible use after free due to an incorrect status check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07299425; Issue ID: ALPS07299425. **CVE ID : CVE-2022-32590**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6923
Out-of-bounds Read	11-Oct-2022	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230794395 **CVE ID : CVE-2022-20412**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6925
Improper Synchronization	07-Oct-2022	6.7	In vdec fmt, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342197; Issue ID: ALPS07342197. **CVE ID : CVE-2022-26473**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6926
Incorrect Calculation of Buffer Size	07-Oct-2022	6.7	In sensorhub, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07129717; Issue ID: ALPS07129717. **CVE ID : CVE-2022-26474**		
Out-of-bounds Write	07-Oct-2022	6.7	In cpu dvfs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07139405; Issue ID: ALPS07139405. **CVE ID : CVE-2022-32592**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6928
Improper Input Validation	07-Oct-2022	6.7	In vowe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138493;	https://corp.mediatek.com/product-security-bulletin/October-2022	O-GOO-ANDR-211022/6929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138493. **CVE ID : CVE-2022-32593**		
N/A	11-Oct-2022	5.5	In start of Threads.cpp, there is a possible way to record audio during a phone call due to a logic error in the code. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235850634 **CVE ID : CVE-2022-20413**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6930
Uncontrolled Resource Consumption	11-Oct-2022	5.5	In addAutomaticZenRule of ZenModeHelper.java, there is a possible permanent degradation of performance due to resource exhaustion. This could lead to local denial of service with User execution privileges needed. User interaction is	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235823407 **CVE ID : CVE-2022-20425**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Oct-2022	5.5	In queryInternal of CallLogProvider.java, there is a possible access to voicemail information due to SQL injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-224771921 **CVE ID : CVE-2022-20351**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6932
Use After Free	07-Oct-2022	5.3	Use after free vulnerability in set_nft_pid and signal_handler function of NFC driver prior to SMR Oct-2022 Release 1	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to perform malicious actions. **CVE ID : CVE-2022-39847**		
Improper Privilege Management	07-Oct-2022	5.3	Improper access control vulnerability in ProfileSharingAccount in Group Sharing prior to versions 13.0.6.15 in Android S(12), 13.0.6.14 in Android R(11) and below allows attackers to identify the device. **CVE ID : CVE-2022-39877**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=10	O-GOO-ANDR-211022/6934
N/A	11-Oct-2022	5	In getInputMethodWindowVisibleHeight of InputMethodManagerService.java, there is a possible way to determine when another app is showing an IME due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12LAndroid ID: A-204906124 **CVE ID : CVE-2022-20394**		
N/A	07-Oct-2022	4.3	Improper access control vulnerability in FACM application prior to SMR Oct-2022 Release 1 allows a local attacker to connect arbitrary AP and Bluetooth devices. **CVE ID : CVE-2022-39855**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6936
N/A	07-Oct-2022	3.3	Improper access control in knox_vpn_policy service prior to SMR Oct-2022 Release 1 allows allows unauthorized read of configuration data. **CVE ID : CVE-2022-39849**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6937
N/A	07-Oct-2022	3.3	Improper access control in mum_container_policy service prior to SMR Oct-2022 Release 1 allows allows unauthorized read of configuration data.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39850		
N/A	07-Oct-2022	3.3	Improper access control vulnerability in CocktailBarService prior to SMR Oct-2022 Release 1 allows local attacker to bind service that require BIND_REMOTEVIEWS permission. **CVE ID : CVE-2022-39851**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6939
N/A	07-Oct-2022	3.3	Improper restriction of broadcasting Intent in MouseNKeyHidDevice prior to SMR Oct-2022 Release 1 leaks MAC address of the connected Bluetooth device. **CVE ID : CVE-2022-36868**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6940
N/A	07-Oct-2022	3.3	Improper access control vulnerability in imsservice application prior to SMR Oct-2022 Release 1 allows local attackers to access call information. **CVE ID : CVE-2022-39856**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=10	O-GOO-ANDR-211022/6941
Exposure of Sensitive Informatio	07-Oct-2022	3.3	Exposure of sensitive information in	https://security.samsungmobile.com/security	O-GOO-ANDR-211022/6942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to an Unauthorized Actor			AT_Distributor prior to SMR Oct-2022 Release 1 allows local attacker to access SerialNo via log. **CVE ID : CVE-2022-39848**	Update.smsb?year=2022&month=10	
Affected Version(s): 12.1					
N/A	11-Oct-2022	8.8	In CarSettings of app packages, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-220741473 **CVE ID : CVE-2022-20429**	https://source.android.com/security/bulletin/aaos/2022-10-01	O-GOO-ANDR-211022/6943
N/A	11-Oct-2022	7.8	In handleFullScreenIntent of StatusBarNotificationActivityStarter.java, there is a possible bypass of the restriction of	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			starting activity from background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-231322873 **CVE ID : CVE-2022-20415**		
Out-of-bounds Write	11-Oct-2022	7.8	In audioTransportsToHal of HidlUtils.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237717857	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20416		
Out-of-bounds Write	11-Oct-2022	7.8	In audioTransportsToHal of HidlUtils.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237288416 **CVE ID : CVE-2022-20417**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6946
N/A	11-Oct-2022	7.8	In setOptions of ActivityRecord.java, there is a possible load any arbitrary Java code into launcher process due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12L Android-13Android ID: A-237290578 **CVE ID : CVE-2022-20419**		
Out-of-bounds Read	11-Oct-2022	7.5	In avrc_ctrl_pars_vendor_rsp of avrc_pars_ct.cc, there is a possible out of bounds read due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-205570663 **CVE ID : CVE-2022-20410**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6948
Out-of-bounds Read	11-Oct-2022	7.5	In pickStartSeq of AAVCAssembler.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-231986464 **CVE ID : CVE-2022-20418**		
Out-of-bounds Read	11-Oct-2022	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230794395 **CVE ID : CVE-2022-20412**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6950
Improper Neutralization of Special Elements used in an SQL Command	11-Oct-2022	5.5	In queryInternal of CallLogProvider.java, there is a possible access to voicemail information due to SQL injection. This could lead to local information	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-224771921 **CVE ID : CVE-2022-20351**		
N/A	11-Oct-2022	5.5	In start of Threads.cpp, there is a possible way to record audio during a phone call due to a logic error in the code. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235850634 **CVE ID : CVE-2022-20413**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6952
Uncontrolled Resource	11-Oct-2022	5.5	In addAutomaticZenRule of	https://source.android.com/se	O-GOO-ANDR-211022/6953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			ZenModeHelper.java, there is a possible permanent degradation of performance due to resource exhaustion. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235823407 **CVE ID : CVE-2022-20425**	curity/bulletin/2022-10-01	
N/A	11-Oct-2022	5	In getInputMethodWindowVisibleHeight of InputMethodManagerService.java, there is a possible way to determine when another app is showing an IME due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-204906124 **CVE ID : CVE-2022-20394**		
Affected Version(s): 13.0					
N/A	11-Oct-2022	7.8	In handleFullScreenIntent of StatusBarNotificationActivityStarter.java, there is a possible bypass of the restriction of starting activity from background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-231322873 **CVE ID : CVE-2022-20415**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	11-Oct-2022	7.8	In audioTransportsToHal of HidlUtils.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237717857 **CVE ID : CVE-2022-20416**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6956
Out-of-bounds Write	11-Oct-2022	7.8	In audioTransportsToHal of HidlUtils.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-237288416 **CVE ID : CVE-2022-20417**		
N/A	11-Oct-2022	7.8	In setOptions of ActivityRecord.java, there is a possible load any arbitrary Java code into launcher process due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-237290578 **CVE ID : CVE-2022-20419**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6958
N/A	11-Oct-2022	7.8	In getBackgroundRestrictionExemptionReason of AppRestrictionController.java, there is a possible way to bypass device policy restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-238377411 **CVE ID : CVE-2022-20420**		
Out-of-bounds Read	11-Oct-2022	7.5	In avrc_ctrl_pars_vendor_rsp of avrc_pars_ct.cc, there is a possible out of bounds read due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-205570663 **CVE ID : CVE-2022-20410**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6960
Out-of-bounds Read	11-Oct-2022	7.5	In pickStartSeq of AAVCAssembler.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-231986464 **CVE ID : CVE-2022-20418**		
Out-of-bounds Read	11-Oct-2022	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230794395 **CVE ID : CVE-2022-20412**	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6962
N/A	11-Oct-2022	5.5	In start of Threads.cpp, there is a possible way to record audio during a phone call due to	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a logic error in the code. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235850634 **CVE ID : CVE-2022-20413**		
Uncontrolled Resource Consumption	11-Oct-2022	5.5	In addAutomaticZenRule of ZenModeHelper.java, there is a possible permanent degradation of performance due to resource exhaustion. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235823407	https://source.android.com/security/bulletin/2022-10-01	O-GOO-ANDR-211022/6964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20425		
Vendor: Huawei					
Product: emui					
Affected Version(s): 11.0.1					
N/A	14-Oct-2022	7.8	The rphone module has a script that can be maliciously modified.Successful exploitation of this vulnerability may cause irreversible programs to be implanted on user devices. **CVE ID : CVE-2022-41576**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6965
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41592**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6966
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consum	O-HUA-EMUI-211022/6967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect the fingerprint service. **CVE ID : CVE-2022-41593**	er.huawei.com/en/support/bulletin/2022/10/	
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41594**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6968
Out-of-bounds Write	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41595**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6969
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consum	O-HUA-EMUI-211022/6970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect the fingerprint service. **CVE ID : CVE-2022-41597**	er.huawei.com/en/support/bulletin/2022/10/	
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41598**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6971
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41600**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6972
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consum	O-HUA-EMUI-211022/6973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect the fingerprint service. **CVE ID : CVE-2022-41601**	er.huawei.com/en/support/bulletin/2022/10/	
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41602**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6974
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41603**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6975
Affected Version(s): 12.0.0					
N/A	14-Oct-2022	7.8	The rphone module has a script that can be maliciously modified.Successful exploitation of this vulnerability may cause irreversible programs to be	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697,	O-HUA-EMUI-211022/6976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implanted on user devices. **CVE ID : CVE-2022-41576**	https://consumer.huawei.com/en/support/bulletin/2022/10/	
Out-of-bounds Read	14-Oct-2022	7.1	The kernel server has a vulnerability of not verifying the length of the data transferred in the user space.Successful exploitation of this vulnerability may cause out-of-bounds read in the kernel, which affects the device confidentiality and availability. **CVE ID : CVE-2022-41577**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6977
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41592**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-EMUI-211022/6978
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-	O-HUA-EMUI-211022/6979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41593**	000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41594**	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	O-HUA-EMUI-211022/6980
Out-of-bounds Write	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41595**	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	O-HUA-EMUI-211022/6981
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-	O-HUA-EMUI-211022/6982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41597**	000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41598**	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	O-HUA-EMUI-211022/6983
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41600**	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	O-HUA-EMUI-211022/6984
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-	O-HUA-EMUI-211022/6985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41601**	000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41602**	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	O-HUA-EMUI-211022/6986
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41603**	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	O-HUA-EMUI-211022/6987
Product: harmonyos					
Affected Version(s): 2.0					
N/A	14-Oct-2022	7.8	The rphone module has a script that can be maliciously modified.Successful	https://device. harmonyos.com /en/docs/secur ity/update/sec	O-HUA-HARM-211022/6988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may cause irreversible programs to be implanted on user devices. **CVE ID : CVE-2022-41576**	urity-bulletins-phones-202210-000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	
Out-of-bounds Read	14-Oct-2022	7.1	The kernel server has a vulnerability of not verifying the length of the data transferred in the user space.Successful exploitation of this vulnerability may cause out-of-bounds read in the kernel, which affects the device confidentiality and availability. **CVE ID : CVE-2022-41577**	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	O-HUA-HARM-211022/6989
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41592**	https://device. harmonyos.com /en/docs/secur ity/update/sec urity-bulletins-phones-202210-000000141609 5697, https://consum er.huawei.com/ en/support/bul letin/2022/10/	O-HUA-HARM-211022/6990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41593**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/6991
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41594**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/6992
Out-of-bounds Write	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41595**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/6993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41597**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/6994
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41598**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/6995
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41600**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/6996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41601**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/6997
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41602**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/6998
Out-of-bounds Read	14-Oct-2022	3.4	The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service. **CVE ID : CVE-2022-41603**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-000000141609 5697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/6999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.1					
Out-of-bounds Read	14-Oct-2022	7.1	The kernel server has a vulnerability of not verifying the length of the data transferred in the user space.Successful exploitation of this vulnerability may cause out-of-bounds read in the kernel, which affects the device confidentiality and availability. **CVE ID : CVE-2022-41577**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-0000001416095697, https://consumer.huawei.com/en/support/bulletin/2022/10/	O-HUA-HARM-211022/7000
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Improper Privilege Management	07-Oct-2022	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information that should only be available to a privileged user. **CVE ID : CVE-2022-36772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/233299, https://www.ibm.com/support/pages/node/6612325	O-IBM-AIX-211022/7001
Insufficient Session Expiration	07-Oct-2022	6.5	IBM InfoSphere Information Server 11.7 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the	https://exchange.xforce.ibmcloud.com/vulnerabilities/236699, https://www.ibm.com/support/pages/node/6823109	O-IBM-AIX-211022/7002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. IBM X-Force ID: 236699. **CVE ID : CVE-2022-41291**		
Vendor: ikuai8					
Product: ikuaios					
Affected Version(s): * Up to (excluding) 3.6.8					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Oct-2022	8.8	iKuai OS v3.6.7 was discovered to contain an authenticated remote code execution (RCE) vulnerability. **CVE ID : CVE-2022-40469**	https://www.ikuai8.com/download.php?n=/3.x/iso/iKuai8_x64_3.6.7_Build202208301257.iso	O-IKU-IKUA-211022/7003
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	07-Oct-2022	8.8	IBM WebSphere Automation for Cloud Pak for Watson AIOps 1.4.2 is vulnerable to cross-site request forgery, caused by improper cookie attribute setting. IBM X-Force ID: 226449. **CVE ID : CVE-2022-22493**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226449, https://www.ibm.com/support/pages/node/6826727	O-LIN-LINU-211022/7004
Exposure of Resource to Wrong Sphere	07-Oct-2022	7.5	IBM QRadar SIEM 7.4 and 7.5 data node rebalancing does not function correctly when using encrypted hosts which could	https://exchange.xforce.ibmcloud.com/vulnerabilities/225889, https://www.ibm.com/support	O-LIN-LINU-211022/7005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in information disclosure. IBM X-Force ID: 225889. **CVE ID : CVE-2022-22480**	/pages/node/6826695	
Improper Privilege Management	07-Oct-2022	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information that should only be available to a privileged user. **CVE ID : CVE-2022-36772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/233299, https://www.ibm.com/support/pages/node/6612325	O-LIN-LINU-211022/7006
Insufficient Session Expiration	07-Oct-2022	6.5	IBM InfoSphere Information Server 11.7 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 236699. **CVE ID : CVE-2022-41291**	https://exchange.xforce.ibmcloud.com/vulnerabilities/236699, https://www.ibm.com/support/pages/node/6823109	O-LIN-LINU-211022/7007
Exposure of Resource to Wrong Sphere	07-Oct-2022	5.5	IBM QRadar SIEM 7.4 and 7.5 could disclose sensitive information via a local service to a privileged user. IBM X-Force ID: 227366. **CVE ID : CVE-2022-30613**	https://exchange.xforce.ibmcloud.com/vulnerabilities/227366, https://www.ibm.com/support/pages/node/6826693	O-LIN-LINU-211022/7008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	07-Oct-2022	5.5	IBM CICS TX 11.1 could allow a local user to cause a denial of service due to improper load handling. IBM X-Force ID: 229437. **CVE ID : CVE-2022-34308**	https://www.ibm.com/support/pages/node/6826647, https://exchange.xforce.ibmcloud.com/vulnerabilities/229437, https://www.ibm.com/support/pages/node/6826645	O-LIN-LINU-211022/7009
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Oct-2022	4.3	A vulnerability classified as problematic has been found in Linux Kernel. This affects the function fib_nh_match of the file net/ipv4/fib_semantics.c of the component IPv4 Handler. The manipulation leads to out-of-bounds read. It is possible to initiate the attack remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-210357 was assigned to this vulnerability. **CVE ID : CVE-2022-3435**	https://vuldb.com/?id.210357, https://lore.kernel.org/netdev/20221005181257.8897-1-dsahern@kernel.org/T/#u,https://vuldb.com/?id.210357	O-LIN-LINU-211022/7010
Affected Version(s): * Up to (excluding) 5.19.7					
Use After Free	09-Oct-2022	5.5	mm/rmap.c in the Linux kernel before 5.19.7 has a use-	https://git.kernel.org/cgit/linux/kernel/git/to	O-LIN-LINU-211022/7011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after-free related to leaf anon_vma double reuse. **CVE ID : CVE-2022-42703**	rvalds/linux.git/commit/?id=2555283eb40df89945557273121e9393ef9b542b, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.7	
Vendor: Linuxfoundation					
Product: yocto					
Affected Version(s): 3.1					
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**	https://corp.mediatek.com/product-security-bulletin/October-2022	O-LIN-YOCT-211022/7012
Affected Version(s): 3.3					
Improper Input Validation	07-Oct-2022	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/October-2022	O-LIN-YOCT-211022/7013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310743; Issue ID: ALPS07310743. **CVE ID : CVE-2022-26475**		
Vendor: mediabridgeproducts					
Product: mlwr-ac1200r_firmware					
Affected Version(s): -					
Improper Authentication	12-Oct-2022	9.8	A vulnerability classified as critical was found in Mediabridge Medialink. This vulnerability affects unknown code of the file /index.asp. The manipulation leads to improper authentication. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-210700. **CVE ID : CVE-2022-3465**	N/A	O-MED-MLWR-211022/7014
Vendor: Microsoft					
Product: azure_rtos_usbx					
Affected Version(s): * Up to (excluding) 6.1.11					
Integer Underflow (Wrap or	10-Oct-2022	9.8	Azure RTOS USBx is a USB host, device, and on-the-go (OTG) embedded	https://github.com/azure-rtos/usbx/security/advisories	O-MIC-AZUR-211022/7015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			stack, fully integrated with Azure RTOS ThreadX and available for all Azure RTOS ThreadX–supported processors. Azure RTOS USBX implementation of host support for USB CDC ECM includes an integer underflow and a buffer overflow in the `_ux_host_class_cdc_ecm_mac_address_get` function which may be potentially exploited to achieve remote code execution or denial of service. Setting mac address string descriptor length to a `0` or `1` allows an attacker to introduce an integer underflow followed (string_length) by a buffer overflow of the `cdc_ecm -> ux_host_class_cdc_ecm_node_id` array. This may allow one to redirect the code execution flow or introduce a denial of service. The fix has been included in USBX release	/GHSA-chpp-5fv9-6368, https://github.com/azure-rtos/usbx/releases/tag/v6.1.12_rel	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[6.1.12](https://github.com/azure-rtos/usbx/releases/tag/v6.1.12_rel). Improved mac address string descriptor length validation to check for unexpectedly small values may be used as a workaround. **CVE ID : CVE-2022-36063**		
Product: storsimple_8010_firmware					
Affected Version(s): -					
N/A	11-Oct-2022	6.8	StorSimple 8000 Series Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38017**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38017	O-MIC-STOR-211022/7016
Product: storsimple_8020_firmware					
Affected Version(s): -					
N/A	11-Oct-2022	6.8	StorSimple 8000 Series Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38017**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38017	O-MIC-STOR-211022/7017
Product: windows					
Affected Version(s): -					
Direct Request ('Forced Browsing')	10-Oct-2022	9.1	A forced browsing vulnerability in Trend Micro Apex One could allow an attacker with access to the Apex	https://success.trendmicro.com/solution/000291645	O-MIC-WIND-211022/7018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			One console on affected installations to escalate privileges and modify certain agent groupings. Please note: an attacker must first obtain the ability to log onto the Apex One web console in order to exploit this vulnerability. **CVE ID : CVE-2022-41746**		
Unquoted Search Path or Element	07-Oct-2022	7.8	Panini Everest Engine 2.0.4 allows unprivileged users to create a file named Everest.exe in the %PROGRAMDATA%\Panini folder. This leads to privilege escalation because a service, running as SYSTEM, uses the unquoted path of %PROGRAMDATA%\Panini\Everest Engine\EverestEngine.exe and therefore a Trojan horse %PROGRAMDATA%\Panini\Everest.exe may be executed instead of the intended vendor-supplied EverestEngine.exe file.	https://www.panini.com/en/news-events/panini-patents-revolutionary-new-%E2%80%9Ceverest%E2%80%9D-architecture	O-MIC-WIND-211022/7019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39959		
Improper Certificate Validation	10-Oct-2022	7.8	An improper certification validation vulnerability in Trend Micro Apex One agents could allow a local attacker to load a DLL file with system service privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41747**	https://success.trendmicro.com/solution/0000291645	O-MIC-WIND-211022/7020
Origin Validation Error	10-Oct-2022	7.8	An origin validation error vulnerability in Trend Micro Apex One agents could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	https://success.trendmicro.com/solution/0000291645	O-MIC-WIND-211022/7021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41749		
N/A	12-Oct-2022	7.5	Multiple Denial-of-Service (DoS) vulnerability was discovered in F-Secure & WithSecure products whereby the aerdl.dll unpacker handler function crashes. This can lead to a possible scanning engine crash. **CVE ID : CVE-2022-28887**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	O-MIC-WIND-211022/7022
Time-of-check Time-of-use (TOCTOU) Race Condition	10-Oct-2022	7	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One Vulnerability Protection integrated component could allow a local attacker to escalate privileges and turn a specific working directory into a mount point on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	https://success.trendmicro.com/solution/0000291645	O-MIC-WIND-211022/7023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41744		
Out-of-bounds Read	10-Oct-2022	7	An Out-of-Bounds access vulnerability in Trend Micro Apex One could allow a local attacker to create a specially crafted message to cause memory corruption on a certain service process which could lead to local privilege escalation on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41745**	https://success.trendmicro.com/solution/0000291645	O-MIC-WIND-211022/7024
Incorrect Default Permissions	10-Oct-2022	6.7	A registry permissions vulnerability in the Trend Micro Apex One Data Loss Prevention (DLP) module could allow a local attacker with administrative credentials to bypass certain elements of the product's anti-tampering mechanisms on affected	https://success.trendmicro.com/solution/0000291645	O-MIC-WIND-211022/7025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installations. Please note: an attacker must first obtain administrative credentials on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-41748**		
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	6.5	The default privileges for the running service Normand Message Buffer in Beckman Coulter Remisol Advance v2.0.12.1 and prior allows non-privileged users to overwrite and manipulate executables and libraries. This allows attackers to access sensitive data. **CVE ID : CVE-2022-26240**	N/A	O-MIC-WIND-211022/7026
Improper Privilege Management	07-Oct-2022	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information that should only be available to a privileged user. **CVE ID : CVE-2022-36772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/233299, https://www.ibm.com/support/pages/node/6612325	O-MIC-WIND-211022/7027
Insufficient Session Expiration	07-Oct-2022	6.5	IBM InfoSphere Information Server 11.7 does not	https://exchange.xforce.ibmcloud.com/vulne	O-MIC-WIND-211022/7028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 236699. **CVE ID : CVE-2022-41291**	rabilities/236699, https://www.ibm.com/support/pages/node/6823109	
Origin Validation Error	06-Oct-2022	6.5	IBM Robotic Process Automation 21.0.0, 21.0.1, 21.0.2, 21.0.3, and 21.0.4 is vulnerable to cross origin resource sharing using the bot api. IBM X-Force ID: 236807. **CVE ID : CVE-2022-41294**	https://exchange.xforce.ibmcloud.com/vulnerabilities/236807, https://www.ibm.com/support/pages/node/6825985	O-MIC-WIND-211022/7029
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-2022	6.1	IBM Robotic Process Automation 21.0.1, 21.0.2, and 21.0.3 for Cloud Pak is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 234291.	https://exchange.xforce.ibmcloud.com/vulnerabilities/234291, https://www.ibm.com/support/pages/node/6826011	O-MIC-WIND-211022/7030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38709		
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	5.5	The default privileges for the running service Normand Remisol Advance Launcher in Beckman Coulter Remisol Advance v2.0.12.1 and prior allows non-privileged users to overwrite and manipulate executables and libraries. This allows attackers to access sensitive data. **CVE ID : CVE-2022-26236**	N/A	O-MIC-WIND-211022/7031
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	5.5	The default privileges for the running service Normand Viewer Service in Beckman Coulter Remisol Advance v2.0.12.1 and prior allows non-privileged users to overwrite and manipulate executables and libraries. This allows attackers to access sensitive data. **CVE ID : CVE-2022-26237**	N/A	O-MIC-WIND-211022/7032
Incorrect Permission Assignmen	06-Oct-2022	5.5	The default privileges for the running service	N/A	O-MIC-WIND-211022/7033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t for Critical Resource			Normand Service Manager in Beckman Coulter Remisol Advance v2.0.12.1 and prior allows non-privileged users to overwrite and manipulate executables and libraries. This allows attackers to access sensitive data. **CVE ID : CVE-2022-26238**		
Incorrect Permission Assignment for Critical Resource	06-Oct-2022	5.5	The default privileges for the running service Normand License Manager in Beckman Coulter Remisol Advance v2.0.12.1 and prior allows unprivileged users to overwrite and manipulate executables and libraries. This allows attackers to access sensitive data. **CVE ID : CVE-2022-26239**	N/A	O-MIC-WIND-211022/7034
Improper Authentication	06-Oct-2022	5.3	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 is vulnerable to man in the middle attacks through manipulation of the client proxy	https://exchange.xforce.ibmcloud.com/vulnerabilities/233575, https://www.ibm.com/support	O-MIC-WIND-211022/7035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration. IBM X-Force ID: 233575. **CVE ID : CVE-2022-36774**	/pages/node/6826013	
Product: windows_10					
Affected Version(s): -					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7036
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7037
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7038
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7039
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-38034**	US/security-guidance/advisory/CVE-2022-38034	
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7041
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7042
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7044
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7045
Concurrent Execution using Shared Resource with Improper Synchroniz	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**		
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7047
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7048
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38042	ory/CVE-2022-38042	
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7050
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7051
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7052
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7053
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7055
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7056
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7058
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7059
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7060
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37979	ory/CVE-2022-37979	
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7062
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7063
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7064
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7066
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7067
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7068
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33645	ory/CVE-2022-33645	
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7070
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7071
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7072
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7073
Concurrent Execution using Shared Resource with Improper Synchroniz	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')					
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7075
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7076
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7077
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7078
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7080
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/7081
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7082
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7083
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7084
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	ory/CVE-2022-38022	
Affected Version(s): 1607					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7086
N/A	11-Oct-2022	8.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38016**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38016	O-MIC-WIND-211022/7087
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7088
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7089
N/A	11-Oct-2022	8.8	Windows Workstation	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	com/en-US/security-guidance/advisory/CVE-2022-38034	
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7091
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7092
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22035		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7094
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7095
Concurrent Execution using Shared Resource with Improper Synchronization	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7097
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7098
Concurrent Execution using Shared Resource with Improper	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**		
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7100
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7101
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7102
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7103
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37986	ory/CVE-2022-37986	
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7105
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7106
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7107
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	US/security-guidance/advisory/CVE-2022-37990	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7109
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7110
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	guidance/advisory/CVE-2022-37994	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/7112
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37979	O-MIC-WIND-211022/7113
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/7115
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7116
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7117
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38038		
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7119
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7120
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7121
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7122
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-34689	
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7124
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7125
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7126
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38021	O-MIC-WIND-211022/7127
Concurrent Execution using Shared	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			**CVE ID : CVE-2022-38027**	guidance/advisory/CVE-2022-38027	
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7129
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7130
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7131
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7132
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability. **CVE ID : CVE-2022-37965**	guidance/advisory/CVE-2022-37965	
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7134
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7135
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/7136
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7137
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7139
Affected Version(s): 1809					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7140
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7141
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-38031. **CVE ID : CVE-2022-37982**		
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7143
N/A	11-Oct-2022	8.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38016**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38016	O-MIC-WIND-211022/7144
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7145
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7146
Concurrent Execution using Shared Resource with Improper Synchronization	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7148
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7149
Concurrent Execution using Shared Resource with	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	ory/CVE-2022-33634	
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7151
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7152
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7154
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7155
Improper Privilege Management	11-Oct-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37970	O-MIC-WIND-211022/7156
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37979	guidance/advisory/CVE-2022-37979	
N/A	11-Oct-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37983**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37983	O-MIC-WIND-211022/7158
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7159
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7160
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7161
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	ory/CVE-2022-37988	
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7163
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7164
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**		
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7166
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7167
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/7168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37995		
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7169
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7170
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/7171
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7173
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038. **CVE ID : CVE-2022-38039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38039	O-MIC-WIND-211022/7174
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7175
N/A	11-Oct-2022	7.8	Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-38050	
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7177
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7178
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7179
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7180
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7182
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7183
N/A	11-Oct-2022	7.5	Web Account Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-38046**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38046	O-MIC-WIND-211022/7184
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38021	O-MIC-WIND-211022/7185
Concurrent Execution using Shared Resource with Improper Synchronization	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7187
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7188
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7189
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7190
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-35770	
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7192
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7193
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7194
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/7195
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7196
N/A	11-Oct-2022	4.3	Windows USB Serial Driver Information	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-38030**	US/security-guidance/advisory/CVE-2022-38030	
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7198
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7199
Affected Version(s): 20h2					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7200
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37982. **CVE ID : CVE-2022-38031**		
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7202
N/A	11-Oct-2022	8.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38016**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38016	O-MIC-WIND-211022/7203
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7204
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7205
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38034	ory/CVE-2022-38034	
Uncontrolled Resource Consumption	11-Oct-2022	8.6	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37998. **CVE ID : CVE-2022-37973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37973	O-MIC-WIND-211022/7207
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7208
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7210
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7211
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7213
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7214
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7216
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7217
N/A	11-Oct-2022	7.8	Windows DHCP Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37980**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37980	O-MIC-WIND-211022/7218
Improper Privilege Management	11-Oct-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37970	O-MIC-WIND-211022/7219
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37979	O-MIC-WIND-211022/7220
N/A	11-Oct-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37983	ory/CVE-2022-37983	
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7222
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7223
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7224
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7226
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7227
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7229
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7230
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/7231
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	ory/CVE-2022-37997	
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7233
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/7234
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7235
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7237
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038. **CVE ID : CVE-2022-38039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38039	O-MIC-WIND-211022/7238
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38050	O-MIC-WIND-211022/7240
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7241
N/A	11-Oct-2022	7.7	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37973. **CVE ID : CVE-2022-37998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37998	O-MIC-WIND-211022/7242
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7243
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7245
N/A	11-Oct-2022	7.5	Web Account Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-38046**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38046	O-MIC-WIND-211022/7246
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7247
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7248
Concurrent Execution using Shared Resource with Improper Synchronization	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38021	O-MIC-WIND-211022/7249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7250
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7251
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7252
Exposure of Resource to Wrong Sphere	11-Oct-2022	6.5	Windows Mixed Reality Developer Tools Information Disclosure Vulnerability. **CVE ID : CVE-2022-37974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37974	O-MIC-WIND-211022/7253
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38033	ory/CVE-2022-38033	
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7255
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7256
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7257
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7258
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/7259
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	guidance/advisory/CVE-2022-38043	
N/A	11-Oct-2022	4.3	Windows USB Serial Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-38030**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38030	O-MIC-WIND-211022/7261
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7262
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7263
Affected Version(s): 21h1					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7265
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7266
N/A	11-Oct-2022	8.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38016**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38016	O-MIC-WIND-211022/7267
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7268
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38040	ory/CVE-2022-38040	
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7270
Uncontrolled Resource Consumption	11-Oct-2022	8.6	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37998. **CVE ID : CVE-2022-37973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37973	O-MIC-WIND-211022/7271
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7272
Concurrent Execution using Shared Resource with Improper Synchroniz	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7274
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7275
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	ory/CVE-2022-41081	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7277
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7278
Concurrent Execution using Shared Resource with Improper Synchronization	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**		
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7280
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7281
N/A	11-Oct-2022	7.8	Windows DHCP Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37980**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37980	O-MIC-WIND-211022/7282
Improper Privilege Management	11-Oct-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37970	O-MIC-WIND-211022/7283
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37979	O-MIC-WIND-211022/7284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37983**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37983	O-MIC-WIND-211022/7285
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7286
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7287
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7288
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**		
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7290
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7291
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**		
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7293
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7294
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/7295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7296
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7297
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/7298
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7299
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7301
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038. **CVE ID : CVE-2022-38039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38039	O-MIC-WIND-211022/7302
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability. **CVE ID : CVE-2022-38044**	guidance/advisory/CVE-2022-38044	
N/A	11-Oct-2022	7.8	Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38050	O-MIC-WIND-211022/7304
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7305
N/A	11-Oct-2022	7.7	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37973. **CVE ID : CVE-2022-37998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37998	O-MIC-WIND-211022/7306
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7307
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Feature Bypass. **CVE ID : CVE-2022-37978**	US/security-guidance/advisory/CVE-2022-37978	
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7309
N/A	11-Oct-2022	7.5	Web Account Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-38046**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38046	O-MIC-WIND-211022/7310
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7311
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7312
Concurrent Execution using Shared Resource with	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			Privilege Vulnerability. **CVE ID : CVE-2022-38021**	ory/CVE-2022-38021	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7314
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7315
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7316
Exposure of Resource to Wrong Sphere	11-Oct-2022	6.5	Windows Mixed Reality Developer Tools Information Disclosure Vulnerability. **CVE ID : CVE-2022-37974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37974	O-MIC-WIND-211022/7317
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	US/security-guidance/advisory/CVE-2022-38033	
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7319
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7320
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7321
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7322
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/7323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7324
N/A	11-Oct-2022	4.3	Windows USB Serial Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-38030**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38030	O-MIC-WIND-211022/7325
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7326
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7327
Affected Version(s): 21h2					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-38045**	US/security-guidance/advisory/CVE-2022-38045	
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7329
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7330
N/A	11-Oct-2022	8.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38016**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38016	O-MIC-WIND-211022/7331
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7333
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7334
Uncontrolled Resource Consumption	11-Oct-2022	8.6	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37998. **CVE ID : CVE-2022-37973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37973	O-MIC-WIND-211022/7335
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7336
Concurrent Execution using	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	US/security-guidance/advisory/CVE-2022-24504	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7338
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7340
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7341
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7342
Concurrent Execution using Shared Resource	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	ory/CVE-2022-38000	
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7344
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7345
N/A	11-Oct-2022	7.8	Windows DHCP Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37980**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37980	O-MIC-WIND-211022/7346
Improper Privilege Management	11-Oct-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37970	O-MIC-WIND-211022/7347
Improper Privilege	11-Oct-2022	7.8	Windows Hyper-V Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Privilege Vulnerability. **CVE ID : CVE-2022-37979**	US/security-guidance/advisory/CVE-2022-37979	
N/A	11-Oct-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37983**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37983	O-MIC-WIND-211022/7349
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7350
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7351
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7352
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	ory/CVE-2022-37988	
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7354
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7355
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	ory/CVE-2022-37991	
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7357
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7358
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/7359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38038, CVE-2022-38039. **CVE ID : CVE-2022-37995**		
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7360
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7361
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/7362
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7363
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	com/en-US/security-guidance/advisory/CVE-2022-38037	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7365
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38039	O-MIC-WIND-211022/7366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38039		
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7367
N/A	11-Oct-2022	7.8	Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38050	O-MIC-WIND-211022/7368
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7369
N/A	11-Oct-2022	7.7	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37973. **CVE ID : CVE-2022-37998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37998	O-MIC-WIND-211022/7370
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33645	ory/CVE-2022-33645	
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7372
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7373
N/A	11-Oct-2022	7.5	Web Account Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-38046**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38046	O-MIC-WIND-211022/7374
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7375
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38021	O-MIC-WIND-211022/7377
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7378
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7379
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7380
Exposure of Resource to Wrong Sphere	11-Oct-2022	6.5	Windows Mixed Reality Developer Tools Information Disclosure Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37974	ory/CVE-2022-37974	
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7382
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7383
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7384
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7385
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7386
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	US/security-guidance/advisory/CVE-2022-37996	
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7388
N/A	11-Oct-2022	4.3	Windows USB Serial Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-38030**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38030	O-MIC-WIND-211022/7389
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7390
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_11					
Affected Version(s): -					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7392
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7393
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7394
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7395
N/A	11-Oct-2022	8.8	Windows Local Security Authority (LSA) Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-38016**	US/security-guidance/advisory/CVE-2022-38016	
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7397
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7398
Uncontrolled Resource Consumption	11-Oct-2022	8.6	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37998. **CVE ID : CVE-2022-37973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37973	O-MIC-WIND-211022/7399
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22035		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7401
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7402
Concurrent Execution using Shared Resource with Improper Synchronization	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7404
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7405
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38042		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7407
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7408
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7409
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-Oct-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37970	O-MIC-WIND-211022/7411
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37979	O-MIC-WIND-211022/7412
N/A	11-Oct-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37983**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37983	O-MIC-WIND-211022/7413
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7414
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7415
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37989. **CVE ID : CVE-2022-37987**	ory/CVE-2022-37987	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7417
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7418
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7420
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7421
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/7423
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7424
N/A	11-Oct-2022	7.8	Windows DHCP Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37980**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37980	O-MIC-WIND-211022/7425
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37999		
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/7427
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7428
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7429
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038. **CVE ID : CVE-2022-38039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38039	O-MIC-WIND-211022/7431
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7432
N/A	11-Oct-2022	7.8	Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38050	O-MIC-WIND-211022/7433
N/A	11-Oct-2022	7.7	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37973.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37998	O-MIC-WIND-211022/7434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37998		
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7435
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7436
N/A	11-Oct-2022	7.5	Internet Key Exchange (IKE) Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-38036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38036	O-MIC-WIND-211022/7437
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7438
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7439
N/A	11-Oct-2022	7.5	Web Account Manager Information	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-38046**	guidance/advisory/CVE-2022-38046	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7441
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38021	O-MIC-WIND-211022/7442
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7443
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38032	ory/CVE-2022-38032	
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7445
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7446
Exposure of Resource to Wrong Sphere	11-Oct-2022	6.5	Windows Mixed Reality Developer Tools Information Disclosure Vulnerability. **CVE ID : CVE-2022-37974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37974	O-MIC-WIND-211022/7447
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7448
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7450
N/A	11-Oct-2022	5.5	Windows Distributed File System (DFS) Information Disclosure Vulnerability. **CVE ID : CVE-2022-38025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38025	O-MIC-WIND-211022/7451
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7452
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/7453
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7454
N/A	11-Oct-2022	4.3	Windows USB Serial Driver Information	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-38030**	guidance/advisory/CVE-2022-38030	
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7456
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7457
Affected Version(s): 22h2					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7458
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37982. **CVE ID : CVE-2022-38031**		
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7460
N/A	11-Oct-2022	8.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38016**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38016	O-MIC-WIND-211022/7461
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7462
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7463
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38034	ory/CVE-2022-38034	
Uncontrolled Resource Consumption	11-Oct-2022	8.6	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37998. **CVE ID : CVE-2022-37973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37973	O-MIC-WIND-211022/7465
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7466
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7468
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7469
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**		
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7471
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7472
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7474
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7475
Improper Privilege Management	11-Oct-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37970	O-MIC-WIND-211022/7476
N/A	11-Oct-2022	7.8	Windows DHCP Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37980**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37980	O-MIC-WIND-211022/7477
N/A	11-Oct-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37983**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37983	O-MIC-WIND-211022/7478
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-37984	
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7480
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7481
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7482
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37987. **CVE ID : CVE-2022-37989**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7484
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7485
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**		
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7487
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/7488
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37979	O-MIC-WIND-211022/7489
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	ory/CVE-2022-37999	
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/7491
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7492
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7493
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038. **CVE ID : CVE-2022-38039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38039	O-MIC-WIND-211022/7495
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7496
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38050	O-MIC-WIND-211022/7498
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7499
N/A	11-Oct-2022	7.7	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37973. **CVE ID : CVE-2022-37998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37998	O-MIC-WIND-211022/7500
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7501
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7503
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7504
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38021	O-MIC-WIND-211022/7505
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7506
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	US/security-guidance/advisory/CVE-2022-38032	
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7508
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7509
Exposure of Resource to Wrong Sphere	11-Oct-2022	6.5	Windows Mixed Reality Developer Tools Information Disclosure Vulnerability. **CVE ID : CVE-2022-37974**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37974	O-MIC-WIND-211022/7510
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7511
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37965		
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7513
N/A	11-Oct-2022	5.5	Windows Distributed File System (DFS) Information Disclosure Vulnerability. **CVE ID : CVE-2022-38025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38025	O-MIC-WIND-211022/7514
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7515
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/7516
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	4.3	Windows USB Serial Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-38030**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38030	O-MIC-WIND-211022/7518
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7519
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7520
Product: windows_7					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37982		
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7522
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7523
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7524
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7525
Concurrent Execution using Shared Resource with Improper Synchroniz	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7527
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7528
Concurrent Execution using Shared Resource	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	ory/CVE-2022-33634	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7530
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7531
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7533
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7534
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7535
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	ory/CVE-2022-37987	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7537
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7538
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7540
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7541
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37994		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7543
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7544
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7545
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**		
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7547
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7548
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7549
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7550
N/A	11-Oct-2022	7.5	Windows Active Directory	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	com/en-US/security-guidance/advisory/CVE-2022-37978	
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7552
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7553
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7554
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7555
Concurrent Execution using Shared Resource	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			**CVE ID : CVE-2022-38029**	ory/CVE-2022-38029	
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7557
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7558
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7559
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7560
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38026	ory/CVE-2022-38026	
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7562
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7563
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7564
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7565
Product: windows_8.1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7566
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7567
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7568
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7569
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38034	ory/CVE-2022-38034	
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7571
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7572
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7573
Concurrent Execution using	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	US/security-guidance/advisory/CVE-2022-30198	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7575
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7577
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7578
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7579
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33635	ory/CVE-2022-33635	
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7581
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7582
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7583
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37999		
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7585
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7586
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7587
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7588
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	ory/CVE-2022-37988	
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7590
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7591
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	ory/CVE-2022-37991	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7593
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7594
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability. **CVE ID : CVE-2022-38044**	US/security-guidance/advisory/CVE-2022-38044	
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7596
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7597
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7598
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7599
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37978	ory/CVE-2022-37978	
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7601
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7602
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7603
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7604
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability. **CVE ID : CVE-2022-37977**	guidance/advisory/CVE-2022-37977	
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7606
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7607
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7608
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7609
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/7611
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7612
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7613
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7614
Product: windows_rt_8.1					
Affected Version(s): -					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	com/en-US/security-guidance/advisory/CVE-2022-38045	
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7616
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7617
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7618
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7620
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7621
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7622
Concurrent Execution using Shared Resource	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	ory/CVE-2022-30198	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7624
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7625
Concurrent Execution	11-Oct-2022	8.1	Windows Point-to-Point Tunneling	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	com/en-US/security-guidance/advisory/CVE-2022-38000	
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7627
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7628
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7630
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7631
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7632
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7634
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7635
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7636
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7637
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**		
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7639
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7640
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7642
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7643
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38044	ory/CVE-2022-38044	
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7645
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7646
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7647
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7648
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7650
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7651
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7652
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7653
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37977	ory/CVE-2022-37977	
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7655
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7656
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7657
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7658
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7659
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	US/security-guidance/advisory/CVE-2022-37996	
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7661
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7662
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7663
Product: windows_server_2008					
Affected Version(s): -					
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38040	ory/CVE-2022-38040	
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7665
Improper Privilege Management	11-Oct-2022	8.8	Active Directory Certificate Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37976	O-MIC-WIND-211022/7666
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7667
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7668
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-38031. **CVE ID : CVE-2022-37982**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7670
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7671
Concurrent Execution using Shared Resource with Improper Synchroniz	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7673
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7674
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	ory/CVE-2022-41081	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7676
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7677
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7678
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-37986**	US/security-guidance/advisory/CVE-2022-37986	
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7680
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7681
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7683
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7684
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7686
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7687
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7688
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7689
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	US/security-guidance/advisory/CVE-2022-38037	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7691
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7692
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38051		
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7694
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7695
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7696
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7697
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7699
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7700
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7701
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7702
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7704
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7705
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7706
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7707
Affected Version(s): r2					
Improper Control of Generation of Code	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	ory/CVE-2022-37982	
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7709
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7710
Improper Privilege Management	11-Oct-2022	8.8	Active Directory Certificate Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37976	O-MIC-WIND-211022/7711
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7712
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37982. **CVE ID : CVE-2022-38031**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7714
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7715
Concurrent Execution using Shared Resource with Improper Synchroniz	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7717
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7718
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38042	ory/CVE-2022-38042	
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7720
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7721
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7723
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7724
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7725
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37989		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7727
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7728
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37993		
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7730
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7731
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7732
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	US/security-guidance/advisory/CVE-2022-38028	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7734
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7735
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7736
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38051		
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7738
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7739
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7740
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7741
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7742
Concurrent Execution using Shared	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			**CVE ID : CVE-2022-38027**	guidance/advisory/CVE-2022-38027	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7744
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7745
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7746
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7748
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7749
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7750
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7751
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7752
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	ory/CVE-2022-38022	
Product: windows_server_2012					
Affected Version(s): -					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7754
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7755
Improper Privilege Management	11-Oct-2022	8.8	Active Directory Certificate Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37976	O-MIC-WIND-211022/7756
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7758
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7759
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7760
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22035		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7762
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7763
Concurrent Execution using Shared Resource with Improper Synchronization	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7765
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7766
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**		
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7768
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7769
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7770
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7771
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	ory/CVE-2022-37987	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7773
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7774
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7776
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7777
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7779
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7780
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7781
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38037		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7783
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7784
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7785
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7787
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7788
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7789
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7790
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7791
Concurrent Execution using	11-Oct-2022	7	Connected User Experiences and Telemetry	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	US/security-guidance/advisory/CVE-2022-38021	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7793
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7794
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7795
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37977		
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7797
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7798
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7799
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7800
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7801
Uncontrolled Resource	11-Oct-2022	4.3	Windows Event Logging Service	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	US/security-guidance/advisory/CVE-2022-37981	
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7803
Affected Version(s): r2					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7804
Improper Privilege Management	11-Oct-2022	8.8	Active Directory Certificate Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37976	O-MIC-WIND-211022/7805
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37982. **CVE ID : CVE-2022-38031**		
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7807
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7808
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7809
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7810
Concurrent Execution using Shared Resource	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	ory/CVE-2022-22035	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7812
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7813
Concurrent Execution	11-Oct-2022	8.1	Windows Point-to-Point Tunneling	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	com/en-US/security-guidance/advisory/CVE-2022-33634	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7815
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41081		
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7817
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7818
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7819
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7821
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7822
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7823
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37989		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7825
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7826
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7827
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	US/security-guidance/advisory/CVE-2022-38037	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7829
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7830
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38028	guidance/advisory/CVE-2022-38028	
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7832
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7833
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7834
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38051		
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7836
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7837
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7838
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7839
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7840
Concurrent Execution using Shared	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Privilege Vulnerability. **CVE ID : CVE-2022-38021**	guidance/advisory/CVE-2022-38021	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7842
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7843
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7844
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38033	ory/CVE-2022-38033	
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7846
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7847
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7848
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7849
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7850
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	US/security-guidance/advisory/CVE-2022-37996	
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7852
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7853
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7854
Product: windows_server_2016					
Affected Version(s): -					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38045	ory/CVE-2022-38045	
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7856
Improper Privilege Management	11-Oct-2022	8.8	Active Directory Certificate Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37976	O-MIC-WIND-211022/7857
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7858
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7859
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-38034**	US/security-guidance/advisory/CVE-2022-38034	
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7861
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7862
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7864
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7865
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7867
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7868
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7870
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37984**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37984	O-MIC-WIND-211022/7871
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7872
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7873
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37989. **CVE ID : CVE-2022-37987**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7875
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37989	O-MIC-WIND-211022/7876
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7878
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7879
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7880
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	ory/CVE-2022-37994	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7882
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7883
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38028	ory/CVE-2022-38028	
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/7885
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7886
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/7887
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37979	O-MIC-WIND-211022/7888
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	guidance/advisory/CVE-2022-38051	
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7890
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7891
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7892
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7893
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38021	O-MIC-WIND-211022/7895
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7896
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/7897
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7898
N/A	11-Oct-2022	6.5	Windows Server Remotely	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	com/en-US/security-guidance/advisory/CVE-2022-38033	
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7900
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7901
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/7902
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7903
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37996	ory/CVE-2022-37996	
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7905
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7906
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/7907
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7908
Product: windows_server_2019					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7909
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7910
N/A	11-Oct-2022	8.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38016**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38016	O-MIC-WIND-211022/7911
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7912
Improper Privilege Management	11-Oct-2022	8.8	Active Directory Certificate Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37976	O-MIC-WIND-211022/7913
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	com/en-US/security-guidance/advisory/CVE-2022-38040	
N/A	11-Oct-2022	8.8	Windows Workstation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38034	O-MIC-WIND-211022/7915
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7916
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7917
Concurrent Execution using Shared	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**	guidance/advisory/CVE-2022-24504	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7919
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7921
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7922
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-38000**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7923
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	ory/CVE-2022-41081	
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7925
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37979	O-MIC-WIND-211022/7926
Improper Privilege Management	11-Oct-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37970	O-MIC-WIND-211022/7927
N/A	11-Oct-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37983**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37983	O-MIC-WIND-211022/7928
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-37984**	US/security-guidance/advisory/CVE-2022-37984	
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7930
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7931
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7932
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	ory/CVE-2022-37989	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7934
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7935
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**	ory/CVE-2022-37993	
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/7937
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/7938
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/7939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/7940
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/7941
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/7942
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/7943
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038. **CVE ID : CVE-2022-38039**	com/en-US/security-guidance/advisory/CVE-2022-38039	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/7945
N/A	11-Oct-2022	7.8	Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38050	O-MIC-WIND-211022/7946
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/7947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-37997. **CVE ID : CVE-2022-38051**		
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7948
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/7949
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/7950
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/7951
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/7952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.5	Web Account Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-38046**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38046	O-MIC-WIND-211022/7953
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/7954
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38021	O-MIC-WIND-211022/7955
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/7956
Concurrent Execution using Shared Resource with	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')				ory/CVE-2022-38029	
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/7958
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/7959
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/7960
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability. **CVE ID : CVE-2022-37977**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37977	O-MIC-WIND-211022/7961
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37965	ory/CVE-2022-37965	
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/7963
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/7964
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/7965
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/7966
N/A	11-Oct-2022	4.3	Windows USB Serial Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-38030**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38030	O-MIC-WIND-211022/7967
Uncontrolled Resource	11-Oct-2022	4.3	Windows Event Logging Service	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-211022/7968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	US/security-guidance/advisory/CVE-2022-37981	
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/7969
Product: windows_server_2022					
Affected Version(s): -					
N/A	11-Oct-2022	9.1	Server Service Remote Protocol Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38045	O-MIC-WIND-211022/7970
N/A	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-37982. **CVE ID : CVE-2022-38031**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38031	O-MIC-WIND-211022/7971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	11-Oct-2022	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-38031. **CVE ID : CVE-2022-37982**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37982	O-MIC-WIND-211022/7972
N/A	11-Oct-2022	8.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38016**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38016	O-MIC-WIND-211022/7973
Improper Privilege Management	11-Oct-2022	8.8	Windows Group Policy Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37975**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975	O-MIC-WIND-211022/7974
Improper Privilege Management	11-Oct-2022	8.8	Active Directory Certificate Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37976**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37976	O-MIC-WIND-211022/7975
N/A	11-Oct-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. **CVE ID : CVE-2022-38040**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38040	O-MIC-WIND-211022/7976
N/A	11-Oct-2022	8.8	Windows Workstation	https://portal.msrc.microsoft.	O-MIC-WIND-211022/7977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38034**	com/en-US/security-guidance/advisory/CVE-2022-38034	
Uncontrolled Resource Consumption	11-Oct-2022	8.6	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37998. **CVE ID : CVE-2022-37973**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37973	O-MIC-WIND-211022/7978
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-22035**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22035	O-MIC-WIND-211022/7979
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24504	O-MIC-WIND-211022/7980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38047, CVE-2022-41081. **CVE ID : CVE-2022-24504**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-30198**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30198	O-MIC-WIND-211022/7981
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081. **CVE ID : CVE-2022-33634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33634	O-MIC-WIND-211022/7982
Concurrent Execution using Shared Resource with Improper Synchroniz	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38047	O-MIC-WIND-211022/7983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-41081. **CVE ID : CVE-2022-38047**		
N/A	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047. **CVE ID : CVE-2022-41081**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41081	O-MIC-WIND-211022/7984
N/A	11-Oct-2022	8.1	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38042**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38042	O-MIC-WIND-211022/7985
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-22035, CVE-2022-24504, CVE-2022-30198, CVE-2022-33634, CVE-2022-38047, CVE-2022-41081.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38000	O-MIC-WIND-211022/7986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38000		
N/A	11-Oct-2022	7.8	Windows GDI+ Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33635**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33635	O-MIC-WIND-211022/7987
N/A	11-Oct-2022	7.8	Windows COM+ Event System Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41033	O-MIC-WIND-211022/7988
Improper Privilege Management	11-Oct-2022	7.8	Windows DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37970**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37970	O-MIC-WIND-211022/7989
Improper Privilege Management	11-Oct-2022	7.8	Windows Hyper-V Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37979	O-MIC-WIND-211022/7990
N/A	11-Oct-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37983**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37983	O-MIC-WIND-211022/7991
N/A	11-Oct-2022	7.8	Windows WLAN Service Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-211022/7992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37984	guidance/advisory/CVE-2022-37984	
N/A	11-Oct-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37986**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37986	O-MIC-WIND-211022/7993
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37989. **CVE ID : CVE-2022-37987**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37987	O-MIC-WIND-211022/7994
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37988**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37988	O-MIC-WIND-211022/7995
N/A	11-Oct-2022	7.8	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/7996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-37987. **CVE ID : CVE-2022-37989**	ory/CVE-2022-37989	
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37990**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37990	O-MIC-WIND-211022/7997
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37991**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37991	O-MIC-WIND-211022/7998
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37993	O-MIC-WIND-211022/7999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			37994, CVE-2022-37999. **CVE ID : CVE-2022-37993**		
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37999. **CVE ID : CVE-2022-37994**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37994	O-MIC-WIND-211022/8000
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-37995**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37995	O-MIC-WIND-211022/8001
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-38051. **CVE ID : CVE-2022-37997**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37997	O-MIC-WIND-211022/8002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	7.8	Windows DHCP Client Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37980**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37980	O-MIC-WIND-211022/8003
N/A	11-Oct-2022	7.8	Windows Group Policy Preference Client Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37993, CVE-2022-37994. **CVE ID : CVE-2022-37999**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37999	O-MIC-WIND-211022/8004
N/A	11-Oct-2022	7.8	Windows Resilient File System Elevation of Privilege. **CVE ID : CVE-2022-38003**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38003	O-MIC-WIND-211022/8005
N/A	11-Oct-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38028**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38028	O-MIC-WIND-211022/8006
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38037	O-MIC-WIND-211022/8007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38022, CVE-2022-38038, CVE-2022-38039. **CVE ID : CVE-2022-38037**		
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38039. **CVE ID : CVE-2022-38038**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38038	O-MIC-WIND-211022/8008
N/A	11-Oct-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38022, CVE-2022-38037, CVE-2022-38038. **CVE ID : CVE-2022-38039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38039	O-MIC-WIND-211022/8009
N/A	11-Oct-2022	7.8	Windows CD-ROM File System Driver Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044	O-MIC-WIND-211022/8010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38044		
N/A	11-Oct-2022	7.8	Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38050	O-MIC-WIND-211022/8011
N/A	11-Oct-2022	7.8	Windows Graphics Component Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37997. **CVE ID : CVE-2022-38051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38051	O-MIC-WIND-211022/8012
N/A	11-Oct-2022	7.7	Windows Local Session Manager (LSM) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-37973. **CVE ID : CVE-2022-37998**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37998	O-MIC-WIND-211022/8013
Uncontrolled Resource Consumption	11-Oct-2022	7.5	Windows TCP/IP Driver Denial of Service Vulnerability. **CVE ID : CVE-2022-33645**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33645	O-MIC-WIND-211022/8014
N/A	11-Oct-2022	7.5	Internet Key Exchange (IKE) Protocol Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/8015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38036	ory/CVE-2022-38036	
N/A	11-Oct-2022	7.5	Windows Active Directory Certificate Services Security Feature Bypass. **CVE ID : CVE-2022-37978**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37978	O-MIC-WIND-211022/8016
N/A	11-Oct-2022	7.5	Windows Secure Channel Denial of Service Vulnerability. **CVE ID : CVE-2022-38041**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38041	O-MIC-WIND-211022/8017
N/A	11-Oct-2022	7.5	Web Account Manager Information Disclosure Vulnerability. **CVE ID : CVE-2022-38046**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38046	O-MIC-WIND-211022/8018
Authentication Bypass by Spoofing	11-Oct-2022	7.5	Windows CryptoAPI Spoofing Vulnerability. **CVE ID : CVE-2022-34689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34689	O-MIC-WIND-211022/8019
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows ALPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38029	O-MIC-WIND-211022/8020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38021**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38021	O-MIC-WIND-211022/8021
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Oct-2022	7	Windows Storage Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38027**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38027	O-MIC-WIND-211022/8022
N/A	11-Oct-2022	6.8	Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-38032**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38032	O-MIC-WIND-211022/8023
N/A	11-Oct-2022	6.5	Windows Server Remotely Accessible Registry Keys Information Disclosure Vulnerability. **CVE ID : CVE-2022-38033**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38033	O-MIC-WIND-211022/8024
N/A	11-Oct-2022	6.5	Local Security Authority Subsystem Service (LSASS) Denial of	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-211022/8025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability. **CVE ID : CVE-2022-37977**	ory/CVE-2022-37977	
Authentication Bypass by Spoofing	11-Oct-2022	6.5	Windows NTLM Spoofing Vulnerability. **CVE ID : CVE-2022-35770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35770	O-MIC-WIND-211022/8026
N/A	11-Oct-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-37965**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37965	O-MIC-WIND-211022/8027
Exposure of Resource to Wrong Sphere	11-Oct-2022	5.5	Windows Graphics Component Information Disclosure Vulnerability. **CVE ID : CVE-2022-37985**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37985	O-MIC-WIND-211022/8028
N/A	11-Oct-2022	5.5	Windows Distributed File System (DFS) Information Disclosure Vulnerability. **CVE ID : CVE-2022-38025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38025	O-MIC-WIND-211022/8029
N/A	11-Oct-2022	5.5	Windows DHCP Client Information Disclosure Vulnerability. **CVE ID : CVE-2022-38026**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38026	O-MIC-WIND-211022/8030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Oct-2022	5.5	Windows Kernel Memory Information Disclosure Vulnerability. **CVE ID : CVE-2022-37996**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37996	O-MIC-WIND-211022/8031
N/A	11-Oct-2022	5.3	Windows Security Support Provider Interface Information Disclosure Vulnerability. **CVE ID : CVE-2022-38043**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38043	O-MIC-WIND-211022/8032
N/A	11-Oct-2022	4.3	Windows USB Serial Driver Information Disclosure Vulnerability. **CVE ID : CVE-2022-38030**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38030	O-MIC-WIND-211022/8033
Uncontrolled Resource Consumption	11-Oct-2022	4.3	Windows Event Logging Service Denial of Service Vulnerability. **CVE ID : CVE-2022-37981**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37981	O-MIC-WIND-211022/8034
N/A	11-Oct-2022	3.3	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37988, CVE-2022-37990, CVE-2022-37991, CVE-2022-37995, CVE-2022-38037, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38022	O-MIC-WIND-211022/8035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			38038, CVE-2022-38039. **CVE ID : CVE-2022-38022**		
Vendor: Nokia					
Product: airframe_bmc_web_gui_r18_firmware					
Affected Version(s): * Up to (excluding) 4.13.00					
Incorrect Authorization	12-Oct-2022	8.8	Multiple Improper Access Control was discovered in Nokia AirFrame BMC Web GUI < R18 Firmware v4.13.00. It does not properly validate requests for access to (or editing of) data and functionality in all endpoints under /#settings/* and /api/settings/*. By not verifying the permissions for access to resources, it allows a potential attacker to view pages, with sensitive data, that are not allowed, and modify system configurations also causing DoS, which should be accessed only by user with administration profile, bypassing all controls (without checking for user identity). **CVE ID : CVE-2022-28866**	N/A	O-NOK-AIRF-211022/8036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Opensuse					
Product: leap					
Affected Version(s): 15.3					
Incorrect Authorization	06-Oct-2022	4.4	A Incorrect Authorization vulnerability in chkstat of SUSE Linux Enterprise Server 12-SP5; openSUSE Leap 15.3, openSUSE Leap 15.4, openSUSE Leap Micro 5.2 did not consider group writable path components, allowing local attackers with access to a group what can write to a location included in the path to a privileged binary to influence path resolution. This issue affects: SUSE Linux Enterprise Server 12-SP5 permissions versions prior to 20170707. openSUSE Leap 15.3 permissions versions prior to 20200127. openSUSE Leap 15.4 permissions versions prior to 20201225. openSUSE Leap Micro 5.2 permissions	https://bugzilla.suse.com/show_bug.cgi?id=1203018	O-OPE-LEAP-211022/8037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20181225. **CVE ID : CVE-2022-31252**		
Affected Version(s): 15.4					
Incorrect Authorization	06-Oct-2022	4.4	A Incorrect Authorization vulnerability in chkstat of SUSE Linux Enterprise Server 12-SP5; openSUSE Leap 15.3, openSUSE Leap 15.4, openSUSE Leap Micro 5.2 did not consider group writable path components, allowing local attackers with access to a group what can write to a location included in the path to a privileged binary to influence path resolution. This issue affects: SUSE Linux Enterprise Server 12-SP5 permissions versions prior to 20170707. openSUSE Leap 15.3 permissions versions prior to 20200127. openSUSE Leap 15.4 permissions versions prior to 20201225. openSUSE Leap	https://bugzilla.suse.com/show_bug.cgi?id=1203018	O-OPE-LEAP-211022/8038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Micro 5.2 permissions versions prior to 20181225. **CVE ID : CVE-2022-31252**		
Product: leap_micro					
Affected Version(s): 5.2					
Incorrect Authorization	06-Oct-2022	4.4	A Incorrect Authorization vulnerability in chkstat of SUSE Linux Enterprise Server 12-SP5; openSUSE Leap 15.3, openSUSE Leap 15.4, openSUSE Leap Micro 5.2 did not consider group writable path components, allowing local attackers with access to a group what can write to a location included in the path to a privileged binary to influence path resolution. This issue affects: SUSE Linux Enterprise Server 12-SP5 permissions versions prior to 20170707. openSUSE Leap 15.3 permissions versions prior to 20200127. openSUSE Leap 15.4 permissions	https://bugzilla.suse.com/show_bug.cgi?id=1203018	O-OPE-LEAP-211022/8039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20201225. openSUSE Leap Micro 5.2 permissions versions prior to 20181225. **CVE ID : CVE-2022-31252**		
Vendor: Paloaltonetworks					
Product: pan-os					
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.24					
Authentication Bypass by Spoofing	12-Oct-2022	8.1	An authentication bypass vulnerability in the Palo Alto Networks PAN-OS 8.1 web interface allows a network-based attacker with specific knowledge of the target firewall or Panorama appliance to impersonate an existing PAN-OS administrator and perform privileged actions. **CVE ID : CVE-2022-0030**	https://security.paloaltonetworks.com/CVE-2022-0030	O-PAL-PAN--211022/8040
Vendor: Siemens					
Product: 6ag1206-2bb00-7ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6AG1-211022/8041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6ag1206-2bs00-7ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6AG1-211022/8042
Product: 6ag1208-0ba00-7ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6AG1-211022/8043
Product: 6ag1216-4bs00-7ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6AG1-211022/8044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5204-0ba00-2gf2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8045
Product: 6gk5204-0ba00-2yf2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8046
Product: 6gk5204-2aa00-2gf2_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8047
Product: 6gk5204-2aa00-2yf2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8048
Product: 6gk5205-3bb00-2ab2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5205-3bb00-2tb2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8050
Product: 6gk5205-3bd00-2ab2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8051
Product: 6gk5205-3bd00-2tb2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5205-3bf00-2ab2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8053
Product: 6gk5205-3bf00-2tb2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8054
Product: 6gk5206-2bb00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5206-2bd00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8056
Product: 6gk5206-2bs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8057
Product: 6gk5206-2bs00-2fc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5206-2gs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8059
Product: 6gk5206-2gs00-2fc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8060
Product: 6gk5206-2gs00-2tc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5206-2rs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8062
Product: 6gk5206-2rs00-5ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8063
Product: 6gk5206-2rs00-5fc2_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8064
Product: 6gk5208-0ba00-2ab2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8065
Product: 6gk5208-0ba00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5208-0ba00-2fc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8067
Product: 6gk5208-0ba00-2tb2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8068
Product: 6gk5208-0ga00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5208-0ga00-2fc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8070
Product: 6gk5208-0ga00-2tc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8071
Product: 6gk5208-0ha00-2as6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5208-0ha00-2es6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8073
Product: 6gk5208-0ha00-2ts6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8074
Product: 6gk5208-0ra00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5208-0ra00-5ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8076
Product: 6gk5208-0ua00-5es6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8077
Product: 6gk5213-3bb00-2ab2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5213-3bb00-2tb2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8079
Product: 6gk5213-3bd00-2ab2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8080
Product: 6gk5213-3bd00-2tb2_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8081
Product: 6gk5213-3bf00-2ab2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8082
Product: 6gk5213-3bf00-2tb2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5216-0ba00-2ab2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8084
Product: 6gk5216-0ba00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8085
Product: 6gk5216-0ba00-2fc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5216-0ba00-2tb2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8087
Product: 6gk5216-0ha00-2as6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8088
Product: 6gk5216-0ha00-2es6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5216-0ha00-2ts6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8090
Product: 6gk5216-0ua00-5es6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8091
Product: 6gk5216-3rs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5216-3rs00-5ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8093
Product: 6gk5216-4bs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8094
Product: 6gk5216-4gs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5216-4gs00-2fc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8096
Product: 6gk5216-4gs00-2tc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8097
Product: 6gk5224-0ba00-2ac2_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8098
Product: 6gk5224-4gs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8099
Product: 6gk5224-4gs00-2fc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5224-4gs00-2tc2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8101
Product: 6gk5324-0ba00-2ar3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8102
Product: 6gk5324-0ba00-3ar3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5326-2qs00-3ar3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8104
Product: 6gk5326-2qs00-3rr3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8105
Product: 6gk5328-4fs00-2ar3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5328-4fs00-2rr3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8107
Product: 6gk5328-4fs00-3ar3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8108
Product: 6gk5328-4fs00-3rr3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5328-4ss00-2ar3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8110
Product: 6gk5328-4ss00-3ar3_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8111
Product: 6gk5408-4gp00-2am2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5408-4gq00-2am2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8113
Product: 6gk5408-8gr00-2am2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8114
Product: 6gk5408-8gs00-2am2_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8115
Product: 6gk5416-4gr00-2am2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8116
Product: 6gk5416-4gs00-2am2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5524-8gr00-2ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8118
Product: 6gk5524-8gr00-3ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8119
Product: 6gk5524-8gr00-4ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5524-8gs00-2ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8121
Product: 6gk5524-8gs00-3ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8122
Product: 6gk5524-8gs00-4ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5526-8gr00-2ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8124
Product: 6gk5526-8gr00-3ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8125
Product: 6gk5526-8gr00-4ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5526-8gs00-2ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8127
Product: 6gk5526-8gs00-3ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8128
Product: 6gk5526-8gs00-4ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5528-0aa00-2ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8130
Product: 6gk5528-0aa00-2hr2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8131
Product: 6gk5528-0ar00-2ar2_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8132
Product: 6gk5528-0ar00-2hr2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8133
Product: 6gk5552-0aa00-2ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5552-0aa00-2hr2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8135
Product: 6gk5552-0ar00-2ar2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8136
Product: 6gk5552-0ar00-2hr2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5622-2gs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8138
Product: 6gk5632-2gs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8139
Product: 6gk5636-2gs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5642-2gs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8141
Product: 6gk5646-2gs00-2ac2_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8142
Product: 6gk5721-1fc00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5721-1fc00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8144
Product: 6gk5722-1fc00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8145
Product: 6gk5722-1fc00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5722-1fc00-0ac0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8147
Product: 6gk5734-1fx00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8148
Product: 6gk5734-1fx00-0aa6_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8149
Product: 6gk5734-1fx00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8150
Product: 6gk5734-1fx00-0ab6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5738-1gy00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8152
Product: 6gk5738-1gy00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8153
Product: 6gk5748-1fc00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5748-1fc00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8155
Product: 6gk5748-1gd00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8156
Product: 6gk5748-1gd00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5748-1gy01-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8158
Product: 6gk5748-1gy01-0ta0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8159
Product: 6gk5761-1fc00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5761-1fc00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8161
Product: 6gk5763-1al00-3aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8162
Product: 6gk5763-1al00-3da0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5763-1al00-7da0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8164
Product: 6gk5766-1ge00-3da0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8165
Product: 6gk5766-1ge00-3db0_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8166
Product: 6gk5766-1ge00-7da0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8167
Product: 6gk5766-1ge00-7db0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5766-1ge00-7ta0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8169
Product: 6gk5766-1ge00-7tb0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8170
Product: 6gk5766-1je00-3da0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5766-1je00-7da0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8172
Product: 6gk5766-1je00-7ta0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8173
Product: 6gk5774-1fx00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5774-1fx00-0aa6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8175
Product: 6gk5774-1fx00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8176
Product: 6gk5774-1fx00-0ab6_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5774-1fx00-0ac0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8178
Product: 6gk5774-1fy00-0ta0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8179
Product: 6gk5774-1fy00-0tb0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5778-1gy00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8181
Product: 6gk5778-1gy00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8182
Product: 6gk5778-1gy00-0ta0_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8183
Product: 6gk5778-1gy00-0tb0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8184
Product: 6gk5786-1fc00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5786-1fc00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8186
Product: 6gk5786-2fc00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8187
Product: 6gk5786-2fc00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5786-2fc00-0ac0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8189
Product: 6gk5786-2fe00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8190
Product: 6gk5786-2fe00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5786-2hc00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8192
Product: 6gk5786-2hc00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8193
Product: 6gk5788-1fc00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5788-1fc00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8195
Product: 6gk5788-1gd00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8196
Product: 6gk5788-1gd00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5788-1gy01-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8198
Product: 6gk5788-2fc00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8199
Product: 6gk5788-2fc00-0ab0_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8200
Product: 6gk5788-2fc00-0ac0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8201
Product: 6gk5788-2gd00-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5788-2gd00-0ab0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8203
Product: 6gk5788-2gd00-0ta0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8204
Product: 6gk5788-2gd00-0tb0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5788-2gd00-0tc0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8206
Product: 6gk5788-2gy01-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8207
Product: 6gk5788-2gy01-0ta0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5788-2hy01-0aa0_firmware					
Affected Version(s): -					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8209
Product: 6gk5804-0ap00-2aa2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8210
Product: 6gk5812-1aa00-2aa2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk5812-1ba00-2aa2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8212
Product: 6gk5816-1aa00-2aa2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8213
Product: 6gk5816-1ba00-2aa2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password	https://cert-portal.siemens.com/productce	O-SIE-6GK5-211022/8214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	rt/pdf/ssa-552702.pdf	
Product: 6gk5826-2ab00-2ab2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8215
Product: 6gk5853-2ea00-2da1_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8216
Product: 6gk5856-2ea00-3aa1_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8217
Product: 6gk5856-2ea00-3da1_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8218
Product: 6gk5874-2aa00-2aa2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 6gk5874-3aa00-2aa2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8220
Product: 6gk5876-3aa02-2ba2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8221
Product: 6gk5876-3aa02-2ea2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31765		
Product: 6gk5876-4aa00-2ba2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8223
Product: 6gk5876-4aa00-2da2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK5-211022/8224
Product: 6gk6108-4am00-2ba2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK6-211022/8225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate their privileges. **CVE ID : CVE-2022-31765**		
Product: 6gk6108-4am00-2da2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Missing Authorization	11-Oct-2022	8.8	Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges. **CVE ID : CVE-2022-31765**	https://cert-portal.siemens.com/productcert/pdf/ssa-552702.pdf	O-SIE-6GK6-211022/8226
Product: 7kg8500-0aa00-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8500-0aa00-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8500-0aa10-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	rt/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8500-0aa10-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Parameter /Argument Delimiters			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All	rt/pdf/ssa-572005.pdf	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41665		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40226		
Product: 7kg8500-0aa30-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8500-0aa30-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa01-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa01-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa02-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa02-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	rt/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa11-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Parameter /Argument Delimiters		🟧	versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All	rt/pdf/ssa-572005.pdf	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41665		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40226		
Product: 7kg8501-0aa11-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa12-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa12-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa31-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa31-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa32-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	rt/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8501-0aa32-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Parameter /Argument Delimiters		🟧	versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All	rt/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41665		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40226		
Product: 7kg8550-0aa00-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa00-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa10-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa10-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa30-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8550-0aa30-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	rt/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa01-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Parameter /Argument Delimiters			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All	rt/pdf/ssa-572005.pdf	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41665		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40226		
Product: 7kg8551-0aa01-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa02-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa02-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa11-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa11-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa12-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	rt/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa12-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All	https://cert-portal.siemens.com/productce	O-SIE-7KG8-211022/8289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Parameter /Argument Delimiters			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All	rt/pdf/ssa-572005.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41665		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40226		
Product: 7kg8551-0aa31-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa31-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa32-0aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: 7kg8551-0aa32-2aa0_firmware					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Parameter /Argument Delimiters	11-Oct-2022	8.8	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the parameter of a specific GET request. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device. **CVE ID : CVE-2022-41665**		
Session Fixation	11-Oct-2022	8.1	A vulnerability has been identified in SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10),	https://cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf	O-SIE-7KG8-211022/8298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login. **CVE ID : CVE-2022-40226**		
Product: apogee_modular_building_controller_firmware					
Affected Version(s): *					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-APOG-211022/8299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: apogee_modular_equiment_controller_firmware					
Affected Version(s): *					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server.	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-APOG-211022/8300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38371		
Product: apogee_pxc_compact_firmware					
Affected Version(s): *					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-APOG-211022/8301
Product: apogee_pxc_modular_firmware					
Affected Version(s): *					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productce	O-SIE-APOG-211022/8302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	rt/pdf/ssa-313313.pdf	
Product: desigo_pxc00-e.d_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxc00-u_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8304
Product: desigo_pxc001-e.d_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of	11-Oct-2022	7.5	A vulnerability has been identified in	https://cert-portal.siemens.	O-SIE-DESI-211022/8305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	
Product: desigo_pxc100-e.d_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxc12-e.d_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server.	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38371		
Product: desigo_pxc128-u_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8308
Product: desigo_pxc200-e.d_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productce	O-SIE-DESI-211022/8309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	rt/pdf/ssa-313313.pdf	
Product: desigo_pxc22-e.d_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxc22.1-e.d_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8311
Product: desigo_pxc36.1-e.d_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of	11-Oct-2022	7.5	A vulnerability has been identified in	https://cert-portal.siemens.	O-SIE-DESI-211022/8312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	
Product: desigo_pxc50-e.d_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**		
Product: desigo_pxc64-u_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server.	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38371		
Product: desigo_pxm20-e_firmware					
Affected Version(s): * Up to (including) 2.3					
Missing Release of Memory after Effective Lifetime	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	O-SIE-DESI-211022/8315
Product: desigo_pxm30-1_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-41					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40182		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code.	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: desigo_pxm30.e_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-41					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40181		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation” web application that interpret and execute Axon language queries, due to the missing validation of anti-	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the “Import Files“ functionality of the “Operation” web application, due to the missing validation of the titles of files	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: desigo_pxm40-1_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-41					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralizat	11-Oct-2022	8.3	A vulnerability has been identified in	https://cert-portal.siemens.	O-SIE-DESI-211022/8331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Encoded URI Schemes in a Web Page			Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting	com/productcert/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions <	https://cert-portal.siemens.com/productce	O-SIE-DESI-211022/8333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41).	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device web application. **CVE ID : CVE-2022-40180**		
Product: desigo_pxm40.e_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-41					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation” web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks.	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1	https://cert-portal.siemens.com/productce	O-SIE-DESI-211022/8342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			(All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the “Import Files“ functionality of the “Operation” web application, due to the missing validation of the titles of files included in the input package. By uploading a	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: desigo_pxm50-1_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-41					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Schemes in a Web Page			Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the “Import Files“ functionality of the “Operation” web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40180		
Product: desigo_pxm50.e_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-41					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option.	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1	https://cert-portal.siemens.com/productce	O-SIE-DESI-211022/8353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			(All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			(All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-DESI-211022/8357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: logo\!8_bm_fs-05_firmware					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Oct-2022	9.8	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not properly validate the structure of TCP packets in several methods. This could allow an attacker to cause buffer overflows, get control over the instruction counter and run custom code.	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	O-SIE-LOGO-211022/8358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36361		
N/A	11-Oct-2022	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not conduct certain validations when interacting with them. This could allow an unauthenticated remote attacker to manipulate the devices IP address, which means the device would not be reachable and could only be recovered by power cycling the device. **CVE ID : CVE-2022-36362**	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	O-SIE-LOGO-211022/8359
Improper Input Validation	11-Oct-2022	5.3	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not properly validate an offset value which can be defined in TCP packets when calling a method. This could allow an attacker to retrieve parts of the content of the memory.	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	O-SIE-LOGO-211022/8360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36363		
Affected Version(s): * Up to (excluding) 8.3					
Insufficient Verification of Data Authenticity	11-Oct-2022	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). Affected devices load firmware updates without checking the authenticity. Furthermore the integrity of the unencrypted firmware is only verified by a non-cryptographic method. This could allow an attacker to manipulate a firmware update and flash it to the device. **CVE ID : CVE-2022-36360**	https://cert-portal.siemens.com/productcert/pdf/ssa-928782.pdf	O-SIE-LOGO-211022/8361
Product: logo\!_8_bm_firmware					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-Oct-2022	9.8	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not properly validate the structure of TCP packets in several methods. This could allow an attacker to cause	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	O-SIE-LOGO-211022/8362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflows, get control over the instruction counter and run custom code. **CVE ID : CVE-2022-36361**		
N/A	11-Oct-2022	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not conduct certain validations when interacting with them. This could allow an unauthenticated remote attacker to manipulate the devices IP address, which means the device would not be reachable and could only be recovered by power cycling the device. **CVE ID : CVE-2022-36362**	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	O-SIE-LOGO-211022/8363
Improper Input Validation	11-Oct-2022	5.3	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions). Affected devices do not properly validate an offset value which can be defined in TCP packets when calling a method.	https://cert-portal.siemens.com/productcert/pdf/ssa-955858.pdf	O-SIE-LOGO-211022/8364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could allow an attacker to retrieve parts of the content of the memory. **CVE ID : CVE-2022-36363**		
Affected Version(s): * Up to (excluding) 8.3					
Insufficient Verification of Data Authenticity	11-Oct-2022	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). Affected devices load firmware updates without checking the authenticity. Furthermore the integrity of the unencrypted firmware is only verified by a non-cryptographic method. This could allow an attacker to manipulate a firmware update and flash it to the device. **CVE ID : CVE-2022-36360**	https://cert-portal.siemens.com/productcert/pdf/ssa-928782.pdf	O-SIE-LOGO-211022/8365
Product: pxg3.w100-1_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-37					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40182		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code.	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation” web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: pxg3.w100-2_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-41					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40181		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the “Import Files“ functionality of the “Operation” web application, due to the missing validation of the titles of files	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41). A Cross-Site Request Forgery exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: pxg3.w200-1_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-37					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralizat	11-Oct-2022	8.3	A vulnerability has been identified in	https://cert-portal.siemens.	O-SIE-PXG3-211022/8381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Encoded URI Schemes in a Web Page			Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting	com/productcert/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the "Operation" web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks. By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions <	https://cert-portal.siemens.com/productce	O-SIE-PXG3-211022/8383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41).	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the "Import Files" functionality of the "Operation" web application, due to the missing validation of the titles of files included in the input package. By uploading a specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in the “Import Files“ functionality of the “Operation” web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device web application. **CVE ID : CVE-2022-40180**		
Product: pxg3.w200-2_firmware					
Affected Version(s): * Up to (excluding) 02.20.126.11-41					
Execution with Unnecessary Privileges	11-Oct-2022	8.8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded Chromium-based browser is launched as root	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the "--no-sandbox" option. Attackers can add arbitrary JavaScript code inside "Operation" graphics and successfully exploit any number of publicly known vulnerabilities against the version of the embedded Chromium-based browser. **CVE ID : CVE-2022-40182**		
Improper Neutralization of Encoded URI Schemes in a Web Page	11-Oct-2022	8.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). The device embedded browser does not prevent interaction with alternative URI schemes when redirected to corresponding resources by web application code. By setting the homepage URI, the favorite URIs, or redirecting embedded browser users via JavaScript code to alternative scheme resources, a remote low privileged attacker can perform a range of attacks against the device, such as read arbitrary files on the filesystem, execute arbitrary JavaScript code in order to steal or manipulate the information on the screen, or trigger denial of service conditions. **CVE ID : CVE-2022-40181**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	11-Oct-2022	8.1	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery exists in endpoints of the “Operation” web application that interpret and execute Axon language queries, due to the missing validation of anti-CSRF tokens or other origin checks.	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			By convincing a victim to click on a malicious link or visit a specifically crafted webpage while logged-in to the device web application, a remote unauthenticated attacker can execute arbitrary Axon queries against the device. **CVE ID : CVE-2022-40179**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Oct-2022	8	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). There exists an Improper Neutralization of Special Elements used in an OS Command with root privileges during a restore operation due to the missing validation of the names of files included in the input package. By restoring a specifically crafted package, a remote low-privileged attacker can execute arbitrary system commands with root privileges on the device, leading to a full compromise. **CVE ID : CVE-2022-40176**		
Exposure of Sensitive Information to an Unauthorized Actor	11-Oct-2022	5.7	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41),	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Endpoints of the "Operation" web application that interpret and execute Axon language queries allow file read access to the device file system with root privileges. By supplying specific I/O related Axon queries, a remote low-privileged attacker can read sensitive files on the device. **CVE ID : CVE-2022-40177**		
Improper Neutralization of	11-Oct-2022	5.4	A vulnerability has been identified in Desigo PXM30-1	https://cert-portal.siemens.com/productce	O-SIE-PXG3-211022/8392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			(All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). Improper Neutralization of Input During Web Page Generation exists in the “Import Files“ functionality of the “Operation” web application, due to the missing validation of the titles of files included in the input package. By uploading a	rt/pdf/ssa-360783.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted graphics package, a remote low-privileged attacker can execute arbitrary JavaScript code. **CVE ID : CVE-2022-40178**		
Cross-Site Request Forgery (CSRF)	11-Oct-2022	5.3	A vulnerability has been identified in Desigo PXM30-1 (All versions < V02.20.126.11-41), Desigo PXM30.E (All versions < V02.20.126.11-41), Desigo PXM40-1 (All versions < V02.20.126.11-41), Desigo PXM40.E (All versions < V02.20.126.11-41), Desigo PXM50-1 (All versions < V02.20.126.11-41), Desigo PXM50.E (All versions < V02.20.126.11-41), PXG3.W100-1 (All versions < V02.20.126.11-37), PXG3.W100-2 (All versions < V02.20.126.11-41), PXG3.W200-1 (All versions < V02.20.126.11-37), PXG3.W200-2 (All versions < V02.20.126.11-41). A Cross-Site Request Forgery	https://cert-portal.siemens.com/productcert/pdf/ssa-360783.pdf	O-SIE-PXG3-211022/8393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists in the "Import Files" functionality of the "Operation" web application due to the missing validation of anti-CSRF tokens or other origin checks. A remote unauthenticated attacker can upload and enable permanent arbitrary JavaScript code into the device just by convincing a victim to visit a specifically crafted webpage while logged-in to the device web application. **CVE ID : CVE-2022-40180**		
Product: ruggedcom_rm1224_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-RUGG-211022/8394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m804pb_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m812-1_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G)	https://cert-portal.siemens.com/productce	O-SIE-SCAL-211022/8396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE	rt/pdf/ssa-697140.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m816-1_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m826-2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m874-2_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G)	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m874-3_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31766		
Product: scalance_m876-3_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_m876-4_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_mum853-1_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_mum856-1_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_s615_firmware					
Affected Version(s): * Up to (excluding) 7.1.2					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_wam763-1_firmware					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_wam766-1_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_wum763-1_firmware					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2),	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2 (All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_wum766-1_firmware					
Affected Version(s): -					
Improper Input Validation	11-Oct-2022	8.6	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (All versions < V7.1.2), RUGGEDCOM RM1224 LTE(4G) NAM (All versions < V7.1.2), SCALANCE M804PB (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M812-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex A) (All versions < V7.1.2), SCALANCE M816-1 ADSL-Router (Annex B) (All versions < V7.1.2), SCALANCE M826-2 SHDSL-Router (All versions < V7.1.2), SCALANCE M874-2	https://cert-portal.siemens.com/productcert/pdf/ssa-697140.pdf	O-SIE-SCAL-211022/8409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V7.1.2), SCALANCE M874-3 (All versions < V7.1.2), SCALANCE M876-3 (EVDO) (All versions < V7.1.2), SCALANCE M876-3 (ROK) (All versions < V7.1.2), SCALANCE M876-4 (EU) (All versions < V7.1.2), SCALANCE M876-4 (NAM) (All versions < V7.1.2), SCALANCE MUM853-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (EU) (All versions < V7.1.2), SCALANCE MUM856-1 (RoW) (All versions < V7.1.2), SCALANCE S615 (All versions < V7.1.2), SCALANCE WAM763-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 (All versions >= V1.1.0), SCALANCE WAM766-1 6GHz (All versions >= V1.1.0), SCALANCE WAM766-1 EEC (All versions >= V1.1.0), SCALANCE WAM766-1 EEC		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions >= V1.1.0), SCALANCE WAM766-1 EEC 6GHz (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM763-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 (All versions >= V1.1.0), SCALANCE WUM766-1 6GHz (All versions >= V1.1.0). Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service and reboot the device thus possibly affecting other network resources. **CVE ID : CVE-2022-31766**		
Product: scalance_x200-4p_irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions	https://cert-portal.siemens.com/productce	O-SIE-SCAL-211022/8410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			< V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2	rt/pdf/ssa-501891.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40631		
Product: scalance_x201-3p_irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x201-3p_irt_pro_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x202-2irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x202-2p_irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x202-2p_irt_pro_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204-2fm_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions	https://cert-portal.siemens.com/productce	O-SIE-SCAL-211022/8416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			< V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2	rt/pdf/ssa-501891.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40631		
Product: scalance_x204-2ld_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204-2ld_ts_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204-2ts_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204-2_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x204irt_pro_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions	https://cert-portal.siemens.com/productce	O-SIE-SCAL-211022/8422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			< V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2	rt/pdf/ssa-501891.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40631		
Product: scalance_x206-1ld_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x206-1_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x208pro_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x208_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x212-2ld_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x212-2_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions	https://cert-portal.siemens.com/productce	O-SIE-SCAL-211022/8428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			< V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2	rt/pdf/ssa-501891.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40631		
Product: scalance_x216_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_x224_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf201-3p_irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf202-2p_irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf204-2ba_irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf204-2_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions	https://cert-portal.siemens.com/productce	O-SIE-SCAL-211022/8434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			< V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2	rt/pdf/ssa-501891.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40631		
Product: scalance_xf204irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf204_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions <		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf206-1_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: scalance_xf208_firmware					
Affected Version(s): * Up to (excluding) 5.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SCAL-211022/8438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions < V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: simatic_drive_controller_cpu_1504d_tf_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_drive_controller_cpu_1507d_tf_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38465		
Product: simatic_et_200_sp_open_controller_cpu_1515sp_pc2_firmware					
Affected Version(s): * Up to (excluding) 21.9					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_et_200_sp_open_controller_cpu_1515sp_pc_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_hmi_comfort_panels_firmware					
Affected Version(s): * Up to (excluding) 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4),	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: simatic_hmi_ktp1200_basic_firmware					
Affected Version(s): * Up to (excluding) 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_hmi_ktp400_basic_firmware					
Affected Version(s): * Up to (excluding) 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels	https://cert-portal.siemens.com/productce	O-SIE-SIMA-211022/8448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition	rt/pdf/ssa-384224.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_hmi_ktp700_basic_firmware					
Affected Version(s): * Up to (excluding) 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_hmi_ktp900_basic_firmware					
Affected Version(s): * Up to (excluding) 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40227		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_hmi_ktp_mobile_panels_firmware					
Affected Version(s): * Up to (excluding) 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5),	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIMA-211022/8454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: simatic_s7-1200_cpu_12_1211c_firmware					
Affected Version(s): * Up to (excluding) 4.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1212c_firmware					
Affected Version(s): * Up to (excluding) 4.5.0					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1212fc_firmware					
Affected Version(s): * Up to (excluding) 4.5.0					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: simatic_s7-1200_cpu_12_1214c_firmware					
Affected Version(s): * Up to (excluding) 4.5.0					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1214fc_firmware					
Affected Version(s): * Up to (excluding) 4.5.0					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1215c_firmware					
Affected Version(s): * Up to (excluding) 4.5.0					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38465		
Product: simatic_s7-1200_cpu_12_1215fc_firmware					
Affected Version(s): * Up to (excluding) 4.5.0					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1200_cpu_12_1217c_firmware					
Affected Version(s): * Up to (excluding) 4.5.0					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1510sp-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1510sp_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1511-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1511t-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1511tf-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1512c-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions <	https://cert-portal.siemens.com/productce	O-SIE-SIMA-211022/8468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication.	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1512sp-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1512spf-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1513-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive	https://cert-portal.siemens.com/productce	O-SIE-SIMA-211022/8471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1513f-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9),	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1513r-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1515-2_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_151511c-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_151511f-1_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: simatic_s7-1500_cpu_1515f-2_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1515r-2_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1515t-2_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38465		
Product: simatic_s7-1500_cpu_1516-3_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1516f-3_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1516pro_f_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1516t-3_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1516tf-3_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1517-3_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1517f-3_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1518-4_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions <	https://cert-portal.siemens.com/productce	O-SIE-SIMA-211022/8487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication.	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1518f-4_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1518hf-4_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1518t-4_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive	https://cert-portal.siemens.com/productce	O-SIE-SIMA-211022/8490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy	rt/pdf/ssa-568427.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_1518tf-4_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9),	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_15pro-2_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-1500_cpu_15prof-2_firmware					
Affected Version(s): * Up to (excluding) 2.9.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: simatic_s7-plcsim_advanced_firmware					
Affected Version(s): * Up to (excluding) 4.0					
Insufficiently Protected Credentials	11-Oct-2022	7.8	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2	https://cert-portal.siemens.com/productcert/pdf/ssa-568427.pdf	O-SIE-SIMA-211022/8494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(incl. SIPLUS variants) (All versions < V21.9), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-PLCSIM Advanced (All versions < V4.0). Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication. **CVE ID : CVE-2022-38465**		
Product: siplus_hmi_ktp1200_basic_firmware					
Affected Version(s): * Up to (excluding) 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIPL-211022/8495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIPL-211022/8496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: siplus_hmi_ktp400_basic_firmware					
Affected Version(s): * Up to (excluding) 17.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIPL-211022/8497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIPL-211022/8498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: siplus_hmi_ktp700_basic_firmware					
Affected Version(s): * Up to (excluding) 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIPL-211022/8499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIPL-211022/8500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: siplus_hmi_ktp900_basic_firmware					
Affected Version(s): * Up to (excluding) 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIPL-211022/8501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Affected Version(s): 17.0					
Improper Input Validation	11-Oct-2022	7.5	A vulnerability has been identified in SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions < V17 Update 4), SIMATIC HMI KTP Mobile Panels (All versions < V17 Update 4), SIMATIC HMI KTP1200 Basic (All versions < V17 Update 5), SIMATIC HMI KTP400 Basic (All versions < V17 Update 5), SIMATIC HMI KTP700 Basic (All versions < V17 Update 5), SIMATIC HMI KTP900 Basic (All versions < V17 Update 5), SIPLUS HMI KTP1200	https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf	O-SIE-SIPL-211022/8502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BASIC (All versions < V17 Update 5), SIPLUS HMI KTP400 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP700 BASIC (All versions < V17 Update 5), SIPLUS HMI KTP900 BASIC (All versions < V17 Update 5). Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets. **CVE ID : CVE-2022-40227**		
Product: siplus_net_scalance_x202-2p_irt_firmware					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Oct-2022	6.1	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT (All versions < V5.5.0), SCALANCE X201-3P IRT PRO (All versions < V5.5.0), SCALANCE X202-	https://cert-portal.siemens.com/productcert/pdf/ssa-501891.pdf	O-SIE-SIPL-211022/8503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2IRT (All versions < V5.5.0), SCALANCE X202-2P IRT (All versions < V5.5.0), SCALANCE X202-2P IRT PRO (All versions < V5.5.0), SCALANCE X204-2 (All versions < V5.2.5), SCALANCE X204-2FM (All versions < V5.2.5), SCALANCE X204-2LD (All versions < V5.2.5), SCALANCE X204-2LD TS (All versions < V5.2.5), SCALANCE X204-2TS (All versions < V5.2.5), SCALANCE X204IRT (All versions < V5.5.0), SCALANCE X204IRT PRO (All versions < V5.5.0), SCALANCE X206-1 (All versions < V5.2.5), SCALANCE X206-1LD (All versions < V5.2.5), SCALANCE X208 (All versions < V5.2.5), SCALANCE X208PRO (All versions < V5.2.5), SCALANCE X212-2 (All versions < V5.2.5), SCALANCE X212-2LD (All versions < V5.2.5), SCALANCE X216 (All versions < V5.2.5), SCALANCE X224 (All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			< V5.2.5), SCALANCE XF201-3P IRT (All versions < V5.5.0), SCALANCE XF202-2P IRT (All versions < V5.5.0), SCALANCE XF204 (All versions < V5.2.5), SCALANCE XF204-2 (All versions < V5.2.5), SCALANCE XF204-2BA IRT (All versions < V5.5.0), SCALANCE XF204IRT (All versions < V5.5.0), SCALANCE XF206-1 (All versions < V5.2.5), SCALANCE XF208 (All versions < V5.2.5), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.0). There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking. **CVE ID : CVE-2022-40631**		
Product: talon_tc_compact_firmware					
Affected Version(s): *					
Missing Release of Memory after	11-Oct-2022	7.5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus ReadyStart V3 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-935500.pdf,	O-SIE-TALO-211022/8504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			versions), Nucleus Source Code (Versions including affected FTP server). The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server. **CVE ID : CVE-2022-38371**	https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf	
Vendor: Suse					
Product: linux_enterprise_server					
Affected Version(s): 12					
Incorrect Authorization	06-Oct-2022	4.4	A Incorrect Authorization vulnerability in chkstat of SUSE Linux Enterprise Server 12-SP5; openSUSE Leap 15.3, openSUSE Leap 15.4, openSUSE Leap Micro 5.2 did not consider group writable path components, allowing local attackers with	https://bugzilla.suse.com/show_bug.cgi?id=1203018	O-SUS-LINU-211022/8505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a group what can write to a location included in the path to a privileged binary to influence path resolution. This issue affects: SUSE Linux Enterprise Server 12-SP5 permissions versions prior to 20170707. openSUSE Leap 15.3 permissions versions prior to 20200127. openSUSE Leap 15.4 permissions versions prior to 20201225. openSUSE Leap Micro 5.2 permissions versions prior to 20181225. **CVE ID : CVE-2022-31252**		
Vendor: Tenda					
Product: ac1206_firmware					
Affected Version(s): 15.03.06.23_multi_td01					
Out-of-bounds Write	12-Oct-2022	7.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 was discovered to contain a stack overflow via the function formWifiBasicSet. **CVE ID : CVE-2022-42079**	N/A	O-TEN-AC12-211022/8506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Oct-2022	7.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 was discovered to contain a heap overflow via sched_start_time parameter. **CVE ID : CVE-2022-42080**	N/A	O-TEN-AC12-211022/8507
Out-of-bounds Write	12-Oct-2022	7.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 was discovered to contain a stack overflow via sched_end_time parameter. **CVE ID : CVE-2022-42081**	N/A	O-TEN-AC12-211022/8508
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolReboot. **CVE ID : CVE-2022-42077**	N/A	O-TEN-AC12-211022/8509
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 is vulnerable to Cross Site Request Forgery (CSRF) via function	N/A	O-TEN-AC12-211022/8510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fromSysToolRestoreSet. **CVE ID : CVE-2022-42078**		
Product: ax1803_firmware					
Affected Version(s): 1.0.0.1_2994_cn_zgyd01_4					
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 is vulnerable to Cross Site Request Forgery (CSRF) via function TendaAteMode. **CVE ID : CVE-2022-42086**	N/A	O-TEN-AX18-211022/8511
Cross-Site Request Forgery (CSRF)	12-Oct-2022	6.5	Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolReboot. **CVE ID : CVE-2022-42087**	N/A	O-TEN-AX18-211022/8512
Vendor: totolink					
Product: nr1800x_firmware					
Affected Version(s): 9.1.0u.6279_b20210910					
Improper Neutralization of Special Elements used in a Command ('Comman	06-Oct-2022	9.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain a command injection vulnerability via	N/A	O-TOT-NR18-211022/8513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			the UploadFirmwareFile function at /cgi-bin/cstecgi.cgi. **CVE ID : CVE-2022-41518**		
Out-of-bounds Write	06-Oct-2022	9.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an unauthenticated stack overflow via the "main" function. **CVE ID : CVE-2022-41522**	N/A	O-TOT-NR18-211022/8514
Out-of-bounds Write	06-Oct-2022	9.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain a command injection vulnerability via the OpModeCfg function at /cgi-bin/cstecgi.cgi. **CVE ID : CVE-2022-41525**	N/A	O-TOT-NR18-211022/8515
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain a stack overflow in the lang parameter in the setLanguageCfg function	N/A	O-TOT-NR18-211022/8516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41517		
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the File parameter in the UploadCustomModule function. **CVE ID : CVE-2022-41520**	N/A	O-TOT-NR18-211022/8517
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the sPort/ePort parameter in the setIpPortFilterRules function. **CVE ID : CVE-2022-41521**	N/A	O-TOT-NR18-211022/8518
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the command parameter in the setTracerouteCfg function.	N/A	O-TOT-NR18-211022/8519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41523		
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the week, sTime, and eTime parameters in the setParentalRules function. **CVE ID : CVE-2022-41524**	N/A	O-TOT-NR18-211022/8520
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the ip parameter in the setDiagnosisCfg function. **CVE ID : CVE-2022-41526**	N/A	O-TOT-NR18-211022/8521
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the pppoeUser parameter in the setOpModeCfg function.	N/A	O-TOT-NR18-211022/8522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41527		
Out-of-bounds Write	06-Oct-2022	8.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain an authenticated stack overflow via the text parameter in the setSmsCfg function. **CVE ID : CVE-2022-41528**	N/A	O-TOT-NR18-211022/8523
Vendor: Vmware					
Product: esxi					
Affected Version(s): * Up to (excluding) 7.0					
NULL Pointer Dereference	07-Oct-2022	6.5	VMware ESXi contains a null-pointer deference vulnerability. A malicious actor with privileges within the VMX process only, may create a denial of service condition on the host. **CVE ID : CVE-2022-31681**	https://www.vmware.com/security/advisories/VMSA-2022-0025.html	O-VMW-ESXI-211022/8524
Affected Version(s): 7.0					
NULL Pointer Dereference	07-Oct-2022	6.5	VMware ESXi contains a null-pointer deference vulnerability. A malicious actor with privileges within the VMX process only, may create a denial of	https://www.vmware.com/security/advisories/VMSA-2022-0025.html	O-VMW-ESXI-211022/8525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service condition on the host. **CVE ID : CVE-2022-31681**		
Vendor: wayos					
Product: lq-04_firmware					
Affected Version(s): 22.03.17					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**	N/A	O-WAY-LQ-0-211022/8526
Product: lq-05_firmware					
Affected Version(s): 22.03.17					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device. This vulnerability is exploitable due to a	N/A	O-WAY-LQ-0-211022/8527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**		
Product: lq-06_firmware					
Affected Version(s): 22.03.17					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**	N/A	O-WAY-LQ-0-211022/8528
Product: lq-07_firmware					
Affected Version(s): 22.03.17					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device. This vulnerability is	N/A	O-WAY-LQ-0-211022/8529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**		
Product: lq-08_firmware					
Affected Version(s): 22.03.17					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device. This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**	N/A	O-WAY-LQ-0-211022/8530
Product: lq-09_firmware					
Affected Version(s): 22.03.17					
Cross-Site Request Forgery (CSRF)	13-Oct-2022	8.1	WAYOS LQ_09 22.03.17V was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to send crafted requests to the server from the affected device.	N/A	O-WAY-LQ-0-211022/8531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is exploitable due to a lack of authentication in the component Usb_upload.htm. **CVE ID : CVE-2022-41489**		
Vendor: wijungle					
Product: u250_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	12-Oct-2022	9.8	WiJungle NGFW Version U250 was discovered to be vulnerable to No Rate Limit attack, allowing the attacker to brute force the admin password leading to Account Take Over. **CVE ID : CVE-2022-33106**	N/A	O-WIJ-U250-211022/8532
Vendor: XEN					
Product: xapi					
Affected Version(s): *					
Uncontrolled Resource Consumption	11-Oct-2022	5.3	XAPI open file limit DoS It is possible for an unauthenticated client on the network to cause XAPI to hit its file-descriptor limit. This causes XAPI to be unable to accept new requests for other (trusted) clients, and blocks XAPI from carrying	https://xenbits.xenproject.org/xsa/advisory-413.txt, http://xenbits.xen.org/xsa/advisory-413.html, http://www.openwall.com/lists/oss-security/2022/10/11/4	O-XEN-XAPI-211022/8533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out any tasks that require the opening of file descriptors. **CVE ID : CVE-2022-33749**		
Product: xen					
Affected Version(s): *					
Uncontrolled Resource Consumption	11-Oct-2022	3.8	Arm: unbounded memory consumption for 2nd-level page tables Certain actions require e.g. removing pages from a guest's P2M (Physical-to-Machine) mapping. When large pages are in use to map guest pages in the 2nd-stage page tables, such a removal operation may incur a memory allocation (to replace a large mapping with individual smaller ones). These memory allocations are taken from the global memory pool. A malicious guest might be able to cause the global memory pool to be exhausted by manipulating its own P2M mappings. **CVE ID : CVE-2022-33747**	https://xenbits.xenproject.org/xsa/advisory-409.txt, http://xenbits.xen.org/xsa/advisory-409.html, http://www.openwall.com/lists/oss-security/2022/10/11/5	O-XEN-XEN-211022/8534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.13.0 Up to (including) 4.16.1					
Uncontrolled Resource Consumption	11-Oct-2022	6.5	P2M pool freeing may take excessively long The P2M pool backing second level address translation for guests may be of significant size. Therefore its freeing may take more time than is reasonable without intermediate preemption checks. Such checking for the need to preempt was so far missing. **CVE ID : CVE-2022-33746**	https://xenbits.xenproject.org/xsa/advisory-410.txt, http://xenbits.xen.org/xsa/advisory-410.html, http://www.openwall.com/lists/oss-security/2022/10/11/3	O-XEN-XEN-211022/8535