National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 - 15 Nov 2022 Vol. 09 No. 21

Table of Content

Vendor	Product	Page Number
AMD	ryzen_3_4300g	641
	ryzen_3_4300ge	641
	ryzen_3_4300u	641
	ryzen_3_5125c	642
	ryzen_3_5400u	642
	ryzen_3_5425c	642
	ryzen_3_5425u	643
	ryzen_5_2500u	643
	ryzen_5_2600	643
	ryzen_5_2600h	644
	ryzen_5_2600x	644
	ryzen_5_2700	644
	ryzen_5_2700x	645
	ryzen_5_3400g	645
	ryzen_5_3450g	645
	ryzen_5_3500u	646
	ryzen_5_3550h	646
	ryzen_5_3580u	646
	ryzen_5_3600	647
	ryzen_5_3600x	647
	ryzen_5_3600xt	647
	ryzen_5_4500u	648
	ryzen_5_4600g	648
	ryzen_5_4600ge	649
	ryzen_5_4600h	649
	ryzen_5_4600u	649
	ryzen_5_5560u	650
	ryzen_5_5600h	650
	ryzen_5_5600hs	650
	ryzen_5_5600u	651
	ryzen_5_5625c	651
	ryzen_5_5625u	651

Vendor	Product	Page Number
Intel	nuc_10_performance_kit_nuc10i5fnk	688
	nuc_10_performance_kit_nuc10i5fnkn	688
	nuc_10_performance_kit_nuc10i5fnkp	689
	nuc_10_performance_kit_nuc10i7fnh	689
	nuc_10_performance_kit_nuc10i7fnhc	690
	nuc_10_performance_kit_nuc10i7fnhn	690
	nuc_10_performance_kit_nuc10i7fnk	691
	nuc_10_performance_kit_nuc10i7fnkn	691
	nuc_10_performance_kit_nuc10i7fnkp	692
	nuc_10_performance_mini_pc_nuc10i3fnhfa	692
	nuc_10_performance_mini_pc_nuc10i3fnhja	693
	nuc_10_performance_mini_pc_nuc10i5fnhca	693
	nuc_10_performance_mini_pc_nuc10i5fnhja	694
	nuc_10_performance_mini_pc_nuc10i5fnkpa	694
	nuc_10_performance_mini_pc_nuc10i7fnhaa	695
	nuc_10_performance_mini_pc_nuc10i7fnhja	695
	nuc_10_performance_mini_pc_nuc10i7fnkpa	696
	nuc_11_compute_element_cm11ebc4w	696
	nuc_11_compute_element_cm11ebi38w	696
	nuc_11_compute_element_cm11ebi58w	697
	nuc_11_compute_element_cm11ebi716w	697
	nuc_11_compute_element_cm11ebv58w	698
	nuc_11_compute_element_cm11ebv716w	698
	nuc_11_performance_kit_nuc11pahi3	699
	nuc_11_performance_kit_nuc11pahi30z	699
	nuc_11_performance_kit_nuc11pahi5	700
	nuc_11_performance_kit_nuc11pahi50z	700
	nuc_11_performance_kit_nuc11pahi7	701
	nuc_11_performance_kit_nuc11pahi70z	701
	nuc_11_performance_kit_nuc11paki3	702
	nuc_11_performance_kit_nuc11paki5	702
	nuc_11_performance_kit_nuc11paki7	703

Vendor	Product	Page Number
mediatek	mt6789	765
	mt6833	769
	mt6853	773
	mt6853t	776
	mt6855	779
	mt6873	783
	mt6875	787
	mt6877	790
	mt6879	793
	mt6880	798
	mt6883	799
	mt6885	802
	mt6889	806
	mt6890	809
	mt6891	810
	mt6893	813
	mt6895	818
	mt6983	824
	mt6985	830
	mt8167	831
	mt8167s	831
	mt8168	831
	mt8173	834
	mt8175	835
	mt8183	836
	mt8185	837
	mt8321	839
	mt8362a	840
	mt8365	840
	mt8385	843
	mt8666	846
	mt8667	847

Vendor	Product	Page Number
Mitsubishielectric	mac-568ifb-e	915
	mac-568ifb2-e	917
	mac-568ifb3-e	918
	mac-576if-e1	920
	mfz-gxt50\/60\/73vfk	925
	mfz-xt50\/60vfk	928
	msxy-fp05\/07\/10\/13\/18\/20\/24vgk-sg1	931
	msy-gp10\/13\/15\/18\/20\/24vfk-sg1	933
	msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-e2	936
	msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-er2	939
	msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-et2	936
	msz-ap22\/25\/35\/42\/50\/60\/71\/80vgkd-a2	944
	msz-ap22\/25\/35\/42\/50\/61\/70\/80vgkd-a1	947
	msz-ap25\/35\/42\/50vgk-e1	950
	msz-ap25\/35\/42\/50vgk-e6	952
	msz-ap25\/35\/42\/50vgk-e7	954
	msz-ap25\/35\/42\/50vgk-e8	957
	msz-ap25\/35\/42\/50vgk-en1	959
	msz-ap25\/35\/42\/50vgk-en2	962
	msz-ap25\/35\/42\/50vgk-en3	965
	msz-ap25\/35\/42\/50vgk-er1	968
	msz-ap25\/35\/42\/50vgk-et1	970
	msz-ap25\/35\/42\/50\/60\/71vgk-e3	973
	msz-ap25\/35\/42\/50\/60\/71vgk-er3	976
	msz-ap25\/35\/42\/50\/60\/71vgk-et3	979

Vendor	Product	Page Number
Mitsubishielectric	msz-ap60\/71vgk-e1	981
	msz-ap60\/71vgk-er1	983
	msz-ap60\/71vgk-et1	985
	msz-ay25\/35\/42\/50vgk-e1	986
	msz-ay25\/35\/42\/50vgk-e6	989
	msz-ay25\/35\/42\/50vgk-er1	992
	msz-ay25\/35\/42\/50vgk-et1	994
	msz-ay25\/35\/42\/50vgk-sc1	997
	msz-ay25\/35\/42\/50vgkp-e6	1000
	msz-ay25\/35\/42\/50vgkp-er1	1003
	msz-ay25\/35\/42\/50vgkp-et1	1005
	msz-ay25\/35\/42\/50vgkp-sc1	1008
	msz-bt20\/25\/35\/50vgk-e1	1011
	msz-bt20\/25\/35\/50vgk-e2	1013
	msz-bt20\/25\/35\/50vgk-e3	1016
	msz-bt20\/25\/35\/50vgk-er1	1019
	msz-bt20\/25\/35\/50vgk-er2	1022
	msz-bt20\/25\/35\/50vgk-et1	1024
	msz-bt20\/25\/35\/50vgk-et2	1027
	msz-bt20\/25\/35\/50vgk-et3	1030
	msz-ef18\/22\/25\/35\/42\/50vgkb-e1	1033
	msz-ef18\/22\/25\/35\/42\/50vgkb-e2	1035
	msz-ef18\/22\/25\/35\/42\/50vgks-e1	1038
	msz-ef18\/22\/25\/35\/42\/50vgks-e2	1041
	msz-ef18\/22\/25\/35\/42\/50vgkw-e1	1043
	msz-ef18\/22\/25\/35\/42\/50vgkw-e2	1046
	msz-ef22\/25\/35\/42\/50vgkb-a1	1049
	msz-ef22\/25\/35\/42\/50vgkb-er1	1052
	msz-ef22\/25\/35\/42\/50vgkb-er2	1054
	msz-ef22\/25\/35\/42\/50vgkb-et1	1057
	msz-ef22\/25\/35\/42\/50vgkb-et2	1060
	msz-ef22\/25\/35\/42\/50vgks-a1	1063

Vendor	Product	Page Number
Mitsubishielectric	msz-ef22\/25\/35\/42\/50vgks-er1	1065
	msz-ef22\/25\/35\/42\/50vgks-er2	1068
	msz-ef22\/25\/35\/42\/50vgks-et1	1071
	msz-ef22\/25\/35\/42\/50vgks-et2	1073
	msz-ef22\/25\/35\/42\/50vgkw-a1	1076
	msz-ef22\/25\/35\/42\/50vgkw-er1	1079
	msz-ef22\/25\/35\/42\/50vgkw-er2	1082
	msz-ef22\/25\/35\/42\/50vgkw-et1	1084
	msz-ef22\/25\/35\/42\/50vgkw-et2	1087
	msz-exa09\/12vak	1090
	msz-eza09\/12vak	1093
	msz-ft20\/25vfk	1095
	msz-ft25\/35\/50vgk-e1	1097
	msz-ft25\/35\/50vgk-e2	1100
	msz-ft25\/35\/50vgk-et1	1102
	msz-ft25\/35\/50vgk-sc1	1105
	msz-ft25\/35\/50vgk-sc2	1108
	msz-fx20\/25vfk	1111
	msz-gzt09\/12\/18vak	1112
	msz-gzy09\/12\/18vfk	1114
	msz-hr25\/35\/42\/50vfk-e6	1117
	msz-hr25\/35\/42\/50\/60\/71vfk-e1	1119
	msz-hr25\/35\/42\/50\/60\/71vfk-er1	1122
	msz-hr25\/35\/42\/50\/60\/71vfk-et1	1125
	msz-ky09\/12\/18vfk	1128
	msz-ln18\/25\/35\/50vg2b-en1	1130
	msz-ln18\/25\/35\/50vg2r-en1	1132
	msz-ln18\/25\/35\/50vg2v-en1	1134
	msz-ln18\/25\/35\/50vg2w-en1	1135
	msz-ln18\/25\/35\/50vg2w-sc1	1137
	msz-ln18\/25\/35\/50\/60vg2b-e1	1140
	msz-ln18\/25\/35\/50\/60vg2b-e2	1141

Vendor	Product	Page Number
Mitsubishielectric	msz-ln18\/25\/35\/50\/60vg2b-e3	1144
	msz-ln18\/25\/35\/50\/60vg2b-et1	1147
	msz-ln18\/25\/35\/50\/60vg2r-e1	1148
	msz-ln18\/25\/35\/50\/60vg2r-e2	1150
	msz-ln18\/25\/35\/50\/60vg2r-e3	1153
	msz-ln18\/25\/35\/50\/60vg2r-et1	1155
	msz-ln18\/25\/35\/50\/60vg2v-e1	1157
	msz-ln18\/25\/35\/50\/60vg2v-e2	1159
	msz-ln18\/25\/35\/50\/60vg2v-e3	1161
	msz-ln18\/25\/35\/50\/60vg2v-et1	1164
	msz-ln18\/25\/35\/50\/60vg2w-e1	1166
	msz-ln18\/25\/35\/50\/60vg2w-e2	1167
	msz-ln18\/25\/35\/50\/60vg2w-e3	1170
	msz-ln18\/25\/35\/50\/60vg2w-er1	1173
	msz-ln18\/25\/35\/50\/60vg2w-er2	1175
	msz-ln18\/25\/35\/50\/60vg2w-et1	1177
	msz-ln18\/25\/35\/50\/60vg2w-et2	1179
	msz-ln18\/25\/35\/50\/60vgb-e1	1182
	msz-ln18\/25\/35\/50\/60vgr-e1	1183
	msz-ln18\/25\/35\/50\/60vgv-e1	1185
	msz-ln18\/25\/35\/50\/60vgw-e1	1187
	msz-ln25\/35\/50vg2b-en2	1188
	msz-ln25\/35\/50vg2b-sc1	1191
	msz-ln25\/35\/50vg2r-en2	1194
	msz-ln25\/35\/50vg2r-sc1	1196
	msz-ln25\/35\/50vg2v-en2	1199
	msz-ln25\/35\/50vg2v-sc1	1202
	msz-ln25\/35\/50vg2w-en2	1205
	msz-ln25\/35\/50\/60vg2b-a1	1207
	msz-ln25\/35\/50\/60vg2b-a2	1209
	msz-ln25\/35\/50\/60vg2b-er1	1212
	msz-ln25\/35\/50\/60vg2b-er2	1213

Vendor	Product	Page Number
Mitsubishielectric	msz-ln25\/35\/50\/60vg2b-er3	1216
	msz-ln25\/35\/50\/60vg2b-et2	1219
	msz-ln25\/35\/50\/60vg2b-et3	1221
	msz-ln25\/35\/50\/60vg2r-a1	1224
	msz-ln25\/35\/50\/60vg2r-a2	1226
	msz-ln25\/35\/50\/60vg2r-er1	1229
	msz-ln25\/35\/50\/60vg2r-er2	1230
	msz-ln25\/35\/50\/60vg2r-er3	1233
	msz-ln25\/35\/50\/60vg2r-et2	1236
	msz-ln25\/35\/50\/60vg2r-et3	1238
	msz-ln25\/35\/50\/60vg2v-a1	1241
	msz-ln25\/35\/50\/60vg2v-a2	1243
	msz-ln25\/35\/50\/60vg2v-er1	1245
	msz-ln25\/35\/50\/60vg2v-er2	1247
	msz-ln25\/35\/50\/60vg2v-er3	1250
	msz-ln25\/35\/50\/60vg2v-et2	1253
	msz-ln25\/35\/50\/60vg2v-et3	1255
	msz-ln25\/35\/50\/60vg2w-er3	1258
	msz-ln25\/35\/50\/60vg2w-et3	1261
	msz-ln25\/35\/50\/60vgb-a1	1263
	msz-ln25\/35\/50\/60vgb-er1	1265
	msz-ln25\/35\/50\/60vgr-a1	1267
	msz-ln25\/35\/50\/60vgr-er1	1268
	msz-ln25\/35\/50\/60vgv-a1	1270
	msz-ln25\/35\/50\/60vgv-er1	1272
	msz-ln25\/35\/50\/60vgw-er1	1273
	msz-rw25\/35\/50vg-e1	1275
	msz-rw25\/35\/50vg-er1	1278
	msz-rw25\/35\/50vg-et1	1280
	msz-rw25\/35\/50vg-sc1	1283
	msz-wx18\/20\/25vfk	1286
	msz-zt09\/12\/18vak	1289

Vendor	Product	Page Number
Siemens	6es7315-2eh14-0ab0	1375
	6es7315-2fj14-0ab0	1378
	6es7315-7tj10-0ab0	1381
	6es7317-2ek14-0ab0	1384
	6es7317-2fk14-0ab0	1387
	6es7317-7tk10-0ab0	1390
	6es7317-7ul10-0ab0	1393
	6es7318-3el01-0ab0	1396
	6es7318-3fl01-0ab0	1399
	7kg9501-0aa01-2aa1	1402
	7kg9501-0aa31-2aa1	1404
	simatic_drive_controller_cpu_1504d_tf	1407
	simatic_drive_controller_cpu_1507d_tf	1410
	simatic_pcs	1413
	simatic_s7-1200_cpu_1211c	1416
	simatic_s7-1200_cpu_1212c	1419
	simatic_s7-1200_cpu_1212fc	1422
	simatic_s7-1200_cpu_1214c	1425
	simatic_s7-1200_cpu_1214fc	1428
	simatic_s7-1200_cpu_1214_fc	1431
	simatic_s7-1200_cpu_1215c	1434
	simatic_s7-1200_cpu_1215fc	1437
	simatic_s7-1200_cpu_1215_fc	1440
	simatic_s7-1200_cpu_1217c	1443
	simatic_s7-1200_cpu_12_1211c	1446
	simatic_s7-1200_cpu_12_1212c	1449
	simatic_s7-1200_cpu_12_1212fc	1452
	simatic_s7-1200_cpu_12_1214c	1455
	simatic_s7-1200_cpu_12_1214fc	1458
	simatic_s7-1200_cpu_12_1215c	1461
	simatic_s7-1200_cpu_12_1215fc	1464
	simatic_s7-1200_cpu_12_1217c	1467

Vendor	Product	Page Number
Siemens	simatic_s7-1500_cpu_1507s	1470
	simatic_s7-1500_cpu_1507s_f	1473
	simatic_s7-1500_cpu_1508s	1476
	simatic_s7-1500_cpu_1508s_f	1479
	simatic_s7-1500_cpu_1510sp	1482
	simatic_s7-1500_cpu_1510sp-1	1485
	simatic_s7-1500_cpu_1511-1	1488
	simatic_s7-1500_cpu_1511-1_pn	1491
	simatic_s7-1500_cpu_1511c	1494
	simatic_s7-1500_cpu_1511c-1	1497
	simatic_s7-1500_cpu_1511f-1	1500
	simatic_s7-1500_cpu_1511f-1_pn	1503
	simatic_s7-1500_cpu_1511t-1	1506
	simatic_s7-1500_cpu_1511tf-1	1509
	simatic_s7-1500_cpu_1512c	1512
	simatic_s7-1500_cpu_1512c-1	1515
	simatic_s7-1500_cpu_1512sp-1	1518
	simatic_s7-1500_cpu_1512spf-1	1521
	simatic_s7-1500_cpu_1513-1	1524
	simatic_s7-1500_cpu_1513-1_pn	1527
	simatic_s7-1500_cpu_1513f-1	1530
	simatic_s7-1500_cpu_1513f-1_pn	1533
	simatic_s7-1500_cpu_1513r-1	1536
	simatic_s7-1500_cpu_1515-2	1539
	simatic_s7-1500_cpu_1515-2_pn	1542
	simatic_s7-1500_cpu_151511c-1	1545
	simatic_s7-1500_cpu_151511f-1	1548
	simatic_s7-1500_cpu_1515f-2	1551
	simatic_s7-1500_cpu_1515f-2_pn	1554
	simatic_s7-1500_cpu_1515r-2	1557
	simatic_s7-1500_cpu_1515t-2	1560
	simatic_s7-1500_cpu_1515tf-2	1563

Vendor	Product	Page Number
Siemens	simatic_s7-1500_cpu_1516-3	1566
	simatic_s7-1500_cpu_1516-3_dp	1569
	simatic_s7-1500_cpu_1516-3_pn	1572
	simatic_s7-1500_cpu_1516-3_pn\/dp	1575
	simatic_s7-1500_cpu_1516f-3	1578
	simatic_s7-1500_cpu_1516f-3_pn\/dp	1581
	simatic_s7-1500_cpu_1516pro-2	1584
	simatic_s7-1500_cpu_1516pro_f	1587
	simatic_s7-1500_cpu_1516t-3	1590
	simatic_s7-1500_cpu_1516tf-3	1593
	simatic_s7-1500_cpu_1517-3	1596
	simatic_s7-1500_cpu_1517-3_dp	1599
	simatic_s7-1500_cpu_1517-3_pn	1602
	simatic_s7-1500_cpu_1517-3_pn\/dp	1605
	simatic_s7-1500_cpu_1517f-3	1608
	simatic_s7-1500_cpu_1517f-3_pn\/dp	1611
	simatic_s7-1500_cpu_1517tf-3	1614
	simatic_s7-1500_cpu_1518	1617
	simatic_s7-1500_cpu_1518-4	1620
	simatic_s7-1500_cpu_1518-4_dp	1623
	simatic_s7-1500_cpu_1518-4_pn	1626
	simatic_s7-1500_cpu_1518-4_pn\/dp	1629
	simatic_s7-1500_cpu_1518-4_pn\/dp_mfp	1632
	simatic_s7-1500_cpu_1518f-4	1635
	simatic_s7-1500_cpu_1518f-4_pn\/dp	1638
	simatic_s7-1500_cpu_1518hf-4	1641
	simatic_s7-1500_cpu_1518t-4	1644
	simatic_s7-1500_cpu_1518tf-4	1647
	simatic_s7-1500_cpu_15pro-2	1650
	simatic_s7-1500_cpu_15prof-2	1653
	simatic_s7-1500_cpu_cpu_1513pro-2	1656
	simatic_s7-1500_cpu_cpu_1513prof-2	1659

Vendor	Product	Page Number
AMD	a6-9220_firmware	1693
	a9-9410_firmware	1693
	a9-9420_firmware	1693
	athlon_gold_3150u_firmware	1694
	athlon_silver_3050u_firmware	1694
	athlon_x4_750_firmware	1694
	athlon_x4_760k_firmware	1695
	athlon_x4_830_firmware	1695
	athlon_x4_835_firmware	1695
	athlon_x4_840_firmware	1696
	athlon_x4_845_firmware	1696
	athlon_x4_860k_firmware	1696
	athlon_x4_870k_firmware	1697
	athlon_x4_880k_firmware	1697
	athlon_x4_940_firmware	1697
	athlon_x4_950_firmware	1698
	athlon_x4_970_firmware	1698
	epyc_7001_firmware	1698
	epyc_7002_firmware	1699
	epyc_7003_firmware	1699
	epyc_7251_firmware	1700
	epyc_7252_firmware	1700
	epyc_7261_firmware	1700
	epyc_7262_firmware	1701
	epyc_7272_firmware	1701
	epyc_7281_firmware	1701
	epyc_7282_firmware	1702
	epyc_72f3_firmware	1702
	epyc_7301_firmware	1702
	epyc_7302p_firmware	1703
	epyc_7302_firmware	1703
	epyc_7313p_firmware	1703

Vendor	Product	Page Number
AMD	epyc_7313_firmware	1704
	epyc_7343_firmware	1704
	epyc_7351p_firmware	1704
	epyc_7351_firmware	1705
	epyc_7352_firmware	1705
	epyc_7371_firmware	1705
	epyc_7373x_firmware	1706
	epyc_7401p_firmware	1706
	epyc_7401_firmware	1707
	epyc_7402p_firmware	1707
	epyc_7402_firmware	1707
	epyc_7413_firmware	1708
	epyc_7443p_firmware	1708
	epyc_7443_firmware	1708
	epyc_7451_firmware	1709
	epyc_7452_firmware	1709
	epyc_7473x_firmware	1709
	epyc_74f3_firmware	1710
	epyc_7501_firmware	1710
	epyc_7502p_firmware	1710
	epyc_7502_firmware	1711
	epyc_7513_firmware	1711
	epyc_7532_firmware	1711
	epyc_7542_firmware	1712
	epyc_7543p_firmware	1712
	epyc_7543_firmware	1712
	epyc_7551p_firmware	1713
	epyc_7551_firmware	1713
	epyc_7552_firmware	1714
	epyc_7573x_firmware	1714
	epyc_75f3_firmware	1714
	epyc_7601_firmware	1715

Vendor	Product	Page Number
AMD	epyc_7642_firmware	1715
	epyc_7643_firmware	1715
	epyc_7662_firmware	1716
	epyc_7663_firmware	1716
	epyc_7702_firmware	1716
	epyc_7713p_firmware	1717
	epyc_7713_firmware	1717
	epyc_7742_firmware	1717
	epyc_7763_firmware	1718
	epyc_7773x_firmware	1718
	epyc_7f32_firmware	1718
	epyc_7f52_firmware	1719
	epyc_7f72_firmware	1719
	epyc_7h12_firmware	1719
	ryzen_3_2200u_firmware	1720
	ryzen_3_2300u_firmware	1720
	ryzen_3_3100_firmware	1721
	ryzen_3_3200u_firmware	1721
	ryzen_3_3250u_firmware	1721
	ryzen_3_3300g_firmware	1722
	ryzen_3_3300u_firmware	1722
	ryzen_3_3300x_firmware	1722
	ryzen_3_4300ge_firmware	1723
	ryzen_3_4300g_firmware	1723
	ryzen_3_4300u_firmware	1723
	ryzen_3_5125c_firmware	1724
	ryzen_3_5400u_firmware	1724
	ryzen_3_5425c_firmware	1724
	ryzen_3_5425u_firmware	1725
	ryzen_5_2500u_firmware	1725
	ryzen_5_2600h_firmware	1725
	ryzen_5_2600x_firmware	1726

Vendor	Product	Page Number
AMD	ryzen_5_2600_firmware	1726
	ryzen_5_2700x_firmware	1726
	ryzen_5_2700_firmware	1727
	ryzen_5_3400g_firmware	1727
	ryzen_5_3450g_firmware	1728
	ryzen_5_3500u_firmware	1728
	ryzen_5_3550h_firmware	1728
	ryzen_5_3580u_firmware	1729
	ryzen_5_3600xt_firmware	1729
	ryzen_5_3600x_firmware	1729
	ryzen_5_3600_firmware	1730
	ryzen_5_4500u_firmware	1730
	ryzen_5_4600ge_firmware	1730
	ryzen_5_4600g_firmware	1731
	ryzen_5_4600h_firmware	1731
	ryzen_5_4600u_firmware	1731
	ryzen_5_5560u_firmware	1732
	ryzen_5_5600hs_firmware	1732
	ryzen_5_5600h_firmware	1732
	ryzen_5_5600u_firmware	1733
	ryzen_5_5625c_firmware	1733
	ryzen_5_5625u_firmware	1733
	ryzen_7_2700u_firmware	1734
	ryzen_7_2700x_firmware	1734
	ryzen_7_2700_firmware	1735
	ryzen_7_2800h_firmware	1735
	ryzen_7_3700u_firmware	1735
	ryzen_7_3700x_firmware	1736
	ryzen_7_3750h_firmware	1736
	ryzen_7_3780u_firmware	1736
	ryzen_7_3800xt_firmware	1737
	ryzen_7_3800x_firmware	1737

Vendor	Product	Page Number
AMD	ryzen_7_4700ge_firmware	1737
	ryzen_7_4700g_firmware	1738
	ryzen_7_4700u_firmware	1738
	ryzen_7_4800h_firmware	1738
	ryzen_7_4800u_firmware	1739
	ryzen_7_5800hs_firmware	1739
	ryzen_7_5800h_firmware	1739
	ryzen_7_5800u_firmware	1740
	ryzen_7_5825c_firmware	1740
	ryzen_7_5825u_firmware	1740
	ryzen_7_pro_3700u_firmware	1741
	ryzen_9_4900h_firmware	1741
	ryzen_9_5900hs_firmware	1742
	ryzen_9_5900hx_firmware	1742
	ryzen_9_5980hs_firmware	1742
	ryzen_9_5980hx_firmware	1743
	ryzen_threadripper_2920x_firmware	1743
	ryzen_threadripper_2950x_firmware	1743
	ryzen_threadripper_2970wx_firmware	1744
	ryzen_threadripper_2990wx_firmware	1744
	ryzen_threadripper_3960x_firmware	1744
	ryzen_threadripper_3970x_firmware	1745
	ryzen_threadripper_3990x_firmware	1745
	ryzen_threadripper_pro_3795wx_firmware	1745
	ryzen_threadripper_pro_3945wx_firmware	1746
	ryzen_threadripper_pro_3955wx_firmware	1746
	ryzen_threadripper_pro_3995wx_firmware	1746
	ryzen_threadripper_pro_5945wx_firmware	1747
	ryzen_threadripper_pro_5955wx_firmware	1747
	ryzen_threadripper_pro_5965wx_firmware	1747
	ryzen_threadripper_pro_5975wx_firmware	1748
	ryzen_threadripper_pro_5995wx_firmware	1748

Vendor	Product	Page Number
Apple	ipados	1749
	ipad_os	1762
	iphone_os	1773
	macos	1809
	mac_os_x	1856
	tvos	1858
	watchos	1876
Avaya	scopia_pathfinder_10_pts_firmware	1898
	scopia_pathfinder_20_pts_firmware	1898
BD	totalys_multiprocessor_firmware	1899
Canonical	ubuntu_linux	1900
Cisco	asyncos	1900
	email_security_appliance_firmware	1914
	secure_email_and_web_manager_firmware	1916
Citrix	application_delivery_controller_firmware	1918
	hypervisor	1922
Debian	debian_linux	1922
Dlink	dir-823g_firmware	1923
Fedoraproject	fedora	1923
Fortinet	fortios	1934
Freebsd	freebsd	1939
Google	android	1940
	chrome_os	2004
HP	hp-ux	2007
Huawei	emui	2008
	harmonyos	2021
IBM	aix	2033
	i	2037
	linux_on_zseries	2039
	z\/os	2039
inhandnetworks	inrouter302_firmware	2040
	ir302_firmware	2040

Vendor	Product	Page Number
Intel	nuc11dbbi7_firmware	2043
	nuc11dbbi9_firmware	2043
	nuc_10_performance_kit_nuc10i3fnhf_firmware	2044
	nuc_10_performance_kit_nuc10i3fnhn_firmware	2044
	nuc_10_performance_kit_nuc10i3fnh_firmware	2045
	nuc_10_performance_kit_nuc10i3fnkn_firmware	2045
	nuc_10_performance_kit_nuc10i3fnk_firmware	2046
	nuc_10_performance_kit_nuc10i5fnhf_firmware	2046
	nuc_10_performance_kit_nuc10i5fnhj_firmware	2047
	nuc_10_performance_kit_nuc10i5fnhn_firmware	2047
	nuc_10_performance_kit_nuc10i5fnh_firmware	2048
	nuc_10_performance_kit_nuc10i5fnkn_firmware	2048
	nuc_10_performance_kit_nuc10i5fnkp_firmware	2049
	nuc_10_performance_kit_nuc10i5fnk_firmware	2049
	nuc_10_performance_kit_nuc10i7fnhc_firmware	2050
	nuc_10_performance_kit_nuc10i7fnhn_firmware	2050
	nuc_10_performance_kit_nuc10i7fnh_firmware	2051
	nuc_10_performance_kit_nuc10i7fnkn_firmware	2051
	nuc_10_performance_kit_nuc10i7fnkp_firmware	2052

Vendor	Product	Page Number
Intel	nuc_10_performance_kit_nuc10i7fnk_firmware	2052
	nuc_10_performance_mini_pc_nuc10i3fnhfa_firmware	2053
	nuc_10_performance_mini_pc_nuc10i3fnhja_firmware	2053
	nuc_10_performance_mini_pc_nuc10i5fnhca_firmware	2054
	nuc_10_performance_mini_pc_nuc10i5fnhja_firmware	2054
	nuc_10_performance_mini_pc_nuc10i5fnkpa_firmware	2055
	nuc_10_performance_mini_pc_nuc10i7fnhaa_firmware	2055
	nuc_10_performance_mini_pc_nuc10i7fnhja_firmware	2056
	nuc_10_performance_mini_pc_nuc10i7fnkpa_firmware	2056
	nuc_11_compute_element_cm11ebc4w_firmware	2057
	nuc_11_compute_element_cm11ebi38w_firmware	2057
	nuc_11_compute_element_cm11ebi58w_firmware	2057
	nuc_11_compute_element_cm11ebi716w_firmware	2058
	nuc_11_compute_element_cm11ebv58w_firmware	2058
	nuc_11_compute_element_cm11ebv716w_firmware	2059
	nuc_11_performance_kit_nuc11pahi30z_firmware	2059
	nuc_11_performance_kit_nuc11pahi3_firmware	2060
	nuc_11_performance_kit_nuc11pahi50z_firmware	2060

Vendor	Product	Page Number
Intel	nuc_11_performance_kit_nuc11pahi5_firmware	2061
	nuc_11_performance_kit_nuc11pahi70z_firmware	2061
	nuc_11_performance_kit_nuc11pahi7_firmware	2062
	nuc_11_performance_kit_nuc11paki3_firmware	2062
	nuc_11_performance_kit_nuc11paki5_firmware	2063
	nuc_11_performance_kit_nuc11paki7_firmware	2063
	nuc_11_performance_mini_pc_nuc11paqi50wa_firmware	2064
	nuc_11_performance_mini_pc_nuc11paqi70qa_firmware	2064
	nuc_11_pro_board_nuc11tnbi30z_firmware	2065
	nuc_11_pro_board_nuc11tnbi50z_firmware	2065
	nuc_11_pro_board_nuc11tnbi70z_firmware	2065
	nuc_11_pro_kit_nuc11tnhi30z_firmware	2066
	nuc_11_pro_kit_nuc11tnhi3_firmware	2066
	nuc_11_pro_kit_nuc11tnhi50z_firmware	2067
	nuc_11_pro_kit_nuc11tnhi5_firmware	2067
	nuc_11_pro_kit_nuc11tnhi70z_firmware	2068
	nuc_11_pro_kit_nuc11tnki30z_firmware	2068
	nuc_11_pro_kit_nuc11tnki50z_firmware	2069
	nuc_11_pro_kit_nuc11tnki70z_firmware	2069
	nuc_8_compute_element_cm8ccb_firmware	2070
	nuc_8_compute_element_cm8i3cb_firmware	2070
	nuc_8_compute_element_cm8i5cb_firmware	2071
	nuc_8_compute_element_cm8i7cb_firmware	2071
	nuc_8_compute_element_cm8pcb_firmware	2071
	nuc_board_de3815tybe_firmware	2072
	nuc_board_nuc5i3mybe_firmware	2072

Vendor	Product	Page Number
Intel	nuc_kit_de3815tykhe_firmware	2073
	nuc_kit_nuc5i3myhe_firmware	2073
	nuc_kit_nuc5i3ryhsn_firmware	2074
	nuc_kit_nuc5i3ryhs_firmware	2075
	nuc_kit_nuc5i3ryh_firmware	2075
	nuc_kit_nuc5i3ryk_firmware	2075
	nuc_kit_nuc5i5ryhs_firmware	2076
	nuc_kit_nuc5i5ryh_firmware	2076
	nuc_kit_nuc5i5ryk_firmware	2077
	nuc_kit_nuc5i7ryh_firmware	2077
	nuc_kit_wireless_adapter_driver_installer	2077
	nuc_m15_laptop_kit_lapbc510_firmware	2079
	nuc_m15_laptop_kit_lapbc710_firmware	2079
	xmm_7560_firmware	2080
Linux	linux_kernel	2083
mediatek	lr12a	2093
	lr13	2094
	nr15	2094
	nr16	2095
Microsoft	azure_rtos_filex	2096
	windows	2097
	windows_10	2106
	windows_11	2158
	windows_7	2173
	windows_8.1	2178
	windows_rt_8.1	2183
	windows_server_2008	2185
	windows_server_2012	2194
	windows_server_2016	2205
	windows_server_2019	2212
	windows_server_2022	2220
mitshubishielectric	mac-507if-e_firmware	2228

Vendor	Product	Page Number
mitshubishielectric	mac-587if-e_firmware	2229
	mac-587if2-e_firmware	2231
	mac-588if-e_firmware	2233
	s-mac-002if_firmware	2234
Mitsubishielectric	ma-ew85s-e_firmware	2236
	ma-ew85s-uk_firmware	2239
	mac-557if-e1_firmware	2243
	mac-557if-e_firmware	2244
	mac-558if-e1_firmware	2246
	mac-558if-e_firmware	2248
	mac-559if-e1_firmware	2249
	mac-559if-e_firmware	2251
	mac-566ifb-e_firmware	2252
	mac-567ifb-e_firmware	2254
	mac-567ifb2-e_firmware	2256
	mac-568if-e_firmware	2257
	mac-568ifb-e_firmware	2259
	mac-568ifb2-e_firmware	2261
	mac-568ifb3-e_firmware	2262
	mac-576if-e1_firmware	2264
	mfz-gxt50\/60\/73vfk_firmware	2269
	mfz-xt50\/60vfk_firmware	2272
	msxy-fp05\/07\/10\/13\/18\/20\/24vgk-sg1_firmware	2274
	msy-gp10\/13\/15\/18\/20\/24vfk-sg1_firmware	2277
	msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-e2_firmware	2280
	msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-er2_firmware	2283

Vendor	Product	Page Number
Mitsubishielectric	msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-et2_firmware	2285
	msz-ap22\/25\/35\/42\/50\/60\/71\/80vgkd-a2_firmware	2288
	msz-ap22\/25\/35\/42\/50\/61\/70\/80vgkd-a1_firmware	2291
	msz-ap25\/35\/42\/50vgk-e1_firmware	2294
	msz-ap25\/35\/42\/50vgk-e6_firmware	2296
	msz-ap25\/35\/42\/50vgk-e7_firmware	2298
	msz-ap25\/35\/42\/50vgk-e8_firmware	2301
	msz-ap25\/35\/42\/50vgk-en1_firmware	2303
	msz-ap25\/35\/42\/50vgk-en2_firmware	2306
	msz-ap25\/35\/42\/50vgk-en3_firmware	2309
	msz-ap25\/35\/42\/50vgk-er1_firmware	2312
	msz-ap25\/35\/42\/50vgk-et1_firmware	2314
	msz-ap25\/35\/42\/50\/60\/71vgk-e3_firmware	2317
	msz-ap25\/35\/42\/50\/60\/71vgk-er3_firmware	2320
	msz-ap25\/35\/42\/50\/60\/71vgk-et3_firmware	2317
	msz-ap60\/71vgk-e1_firmware	2325
	msz-ap60\/71vgk-er1_firmware	2327
	msz-ap60\/71vgk-et1_firmware	2328
	msz-ay25\/35\/42\/50vgk-e1_firmware	2330
	msz-ay25\/35\/42\/50vgk-e6_firmware	2333
	msz-ay25\/35\/42\/50vgk-er1_firmware	2336
	msz-ay25\/35\/42\/50vgk-et1_firmware	2338
	msz-ay25\/35\/42\/50vgk-sc1_firmware	2341
	msz-ay25\/35\/42\/50vgkp-e6_firmware	2344
	msz-ay25\/35\/42\/50vgkp-er1_firmware	2347
	msz-ay25\/35\/42\/50vgkp-et1_firmware	2349

Vendor	Product	Page Number
Mitsubishielectric	msz-ay25\/35\/42\/50vgkp-sc1_firmware	2352
	msz-bt20\/25\/35\/50vgk-e1_firmware	2355
	msz-bt20\/25\/35\/50vgk-e2_firmware	2357
	msz-bt20\/25\/35\/50vgk-e3_firmware	2360
	msz-bt20\/25\/35\/50vgk-er1_firmware	2363
	msz-bt20\/25\/35\/50vgk-er2_firmware	2366
	msz-bt20\/25\/35\/50vgk-et1_firmware	2368
	msz-bt20\/25\/35\/50vgk-et2_firmware	2371
	msz-bt20\/25\/35\/50vgk-et3_firmware	2374
	msz-ef18\/22\/25\/35\/42\/50vgkb-e1_firmware	2377
	msz-ef18\/22\/25\/35\/42\/50vgkb-e2_firmware	2379
	msz-ef18\/22\/25\/35\/42\/50vgks-e1_firmware	2382
	msz-ef18\/22\/25\/35\/42\/50vgks-e2_firmware	2385
	msz-ef18\/22\/25\/35\/42\/50vgkw-e1_firmware	2387
	msz-ef18\/22\/25\/35\/42\/50vgkw-e2_firmware	2390
	msz-ef22\/25\/35\/42\/50vgkb-a1_firmware	2393
	msz-ef22\/25\/35\/42\/50vgkb-er1_firmware	2396
	msz-ef22\/25\/35\/42\/50vgkb-er2_firmware	2398
	msz-ef22\/25\/35\/42\/50vgkb-et1_firmware	2401
	msz-ef22\/25\/35\/42\/50vgkb-et2_firmware	2404
	msz-ef22\/25\/35\/42\/50vgks-a1_firmware	2407
	msz-ef22\/25\/35\/42\/50vgks-er1_firmware	2409

Vendor	Product	Page Number
Mitsubishielectric	msz-ef22\/25\/35\/42\/50vgks-er2_firmware	2412
	msz-ef22\/25\/35\/42\/50vgks-et1_firmware	2415
	msz-ef22\/25\/35\/42\/50vgks-et2_firmware	2417
	msz-ef22\/25\/35\/42\/50vgkw-a1_firmware	2420
	msz-ef22\/25\/35\/42\/50vgkw-er1_firmware	2423
	msz-ef22\/25\/35\/42\/50vgkw-er2_firmware	2426
	msz-ef22\/25\/35\/42\/50vgkw-et1_firmware	2428
	msz-ef22\/25\/35\/42\/50vgkw-et2_firmware	2431
	msz-exa09\/12vak_firmware	2434
	msz-eza09\/12vak_firmware	2437
	msz-ft20\/25vfk_firmware	2439
	msz-ft25\/35\/50vgk-e1_firmware	2441
	msz-ft25\/35\/50vgk-e2_firmware	2444
	msz-ft25\/35\/50vgk-et1_firmware	2446
	msz-ft25\/35\/50vgk-sc1_firmware	2449
	msz-ft25\/35\/50vgk-sc2_firmware	2452
	msz-fx20\/25vfk_firmware	2455
	msz-gzt09\/12\/18vak_firmware	2456
	msz-gzy09\/12\/18vfk_firmware	2458
	msz-hr25\/35\/42\/50vfk-e6_firmware	2461
	msz-hr25\/35\/42\/50\/60\/71vfk-e1_firmware	2463
	msz-hr25\/35\/42\/50\/60\/71vfk-er1_firmware	2466
	msz-hr25\/35\/42\/50\/60\/71vfk-et1_firmware	2469
	msz-ky09\/12\/18vfk_firmware	2472

Vendor	Product	Page Number
Mitsubishielectric	msz-ln18\/25\/35\/50vg2b-en1_firmware	2474
	msz-ln18\/25\/35\/50vg2r-en1_firmware	2476
	msz-ln18\/25\/35\/50vg2v-en1_firmware	2478
	msz-ln18\/25\/35\/50vg2w-en1_firmware	2479
	msz-ln18\/25\/35\/50vg2w-sc1_firmware	2481
	msz-ln18\/25\/35\/50\/60vg2b-e1_firmware	2484
	msz-ln18\/25\/35\/50\/60vg2b-e2_firmware	2485
	msz-ln18\/25\/35\/50\/60vg2b-e3_firmware	2488
	msz-ln18\/25\/35\/50\/60vg2b-et1_firmware	2491
	msz-ln18\/25\/35\/50\/60vg2r-e1_firmware	2492
	msz-ln18\/25\/35\/50\/60vg2r-e2_firmware	2494
	msz-ln18\/25\/35\/50\/60vg2r-e3_firmware	2497
	msz-ln18\/25\/35\/50\/60vg2r-et1_firmware	2499
	msz-ln18\/25\/35\/50\/60vg2v-e1_firmware	2501
	msz-ln18\/25\/35\/50\/60vg2v-e2_firmware	2503
	msz-ln18\/25\/35\/50\/60vg2v-e3_firmware	2505
	msz-ln18\/25\/35\/50\/60vg2v-et1_firmware	2508
	msz-ln18\/25\/35\/50\/60vg2w-e1_firmware	2510
	msz-ln18\/25\/35\/50\/60vg2w-e2_firmware	2511
	msz-ln18\/25\/35\/50\/60vg2w-e3_firmware	2514
	msz-ln18\/25\/35\/50\/60vg2w-er1_firmware	2517

Vendor	Product	Page Number
Mitsubishielectric	msz-ln18\/25\/35\/50\/60vg2w-er2_firmware	2519
	msz-ln18\/25\/35\/50\/60vg2w-et1_firmware	2521
	msz-ln18\/25\/35\/50\/60vg2w-et2_firmware	2523
	msz-ln18\/25\/35\/50\/60vgb-e1_firmware	2526
	msz-ln18\/25\/35\/50\/60vgr-e1_firmware	2527
	msz-ln18\/25\/35\/50\/60vgv-e1_firmware	2529
	msz-ln18\/25\/35\/50\/60vgw-e1_firmware	2531
	msz-ln25\/35\/50vg2b-en2_firmware	2532
	msz-ln25\/35\/50vg2b-sc1_firmware	2535
	msz-ln25\/35\/50vg2r-en2_firmware	2538
	msz-ln25\/35\/50vg2r-sc1_firmware	2540
	msz-ln25\/35\/50vg2v-en2_firmware	2543
	msz-ln25\/35\/50vg2v-sc1_firmware	2546
	msz-ln25\/35\/50vg2w-en2_firmware	2549
	msz-ln25\/35\/50\/60vg2b-a1_firmware	2551
	msz-ln25\/35\/50\/60vg2b-a2_firmware	2553
	msz-ln25\/35\/50\/60vg2b-er1_firmware	2556
	msz-ln25\/35\/50\/60vg2b-er2_firmware	2557
	msz-ln25\/35\/50\/60vg2b-er3_firmware	2560
	msz-ln25\/35\/50\/60vg2b-et2_firmware	2563
	msz-ln25\/35\/50\/60vg2b-et3_firmware	2565
	msz-ln25\/35\/50\/60vg2r-a1_firmware	2568
	msz-ln25\/35\/50\/60vg2r-a2_firmware	2570
	msz-ln25\/35\/50\/60vg2r-er1_firmware	2573
	msz-ln25\/35\/50\/60vg2r-er2_firmware	2574
	msz-ln25\/35\/50\/60vg2r-er3_firmware	2577
	msz-ln25\/35\/50\/60vg2r-et2_firmware	2580
	msz-ln25\/35\/50\/60vg2r-et3_firmware	2582
	msz-ln25\/35\/50\/60vg2v-a1_firmware	2585
	msz-ln25\/35\/50\/60vg2v-a2_firmware	2587

Vendor	Product	Page Number
Mitsubishielectric	msz-ln25\/35\/50\/60vg2v-er1_firmware	2589
	msz-ln25\/35\/50\/60vg2v-er2_firmware	2591
	msz-ln25\/35\/50\/60vg2v-er3_firmware	2594
	msz-ln25\/35\/50\/60vg2v-et2_firmware	2597
	msz-ln25\/35\/50\/60vg2v-et3_firmware	2599
	msz-ln25\/35\/50\/60vg2w-er3_firmware	2602
	msz-ln25\/35\/50\/60vg2w-et3_firmware	2605
	msz-ln25\/35\/50\/60vgb-a1_firmware	2607
	msz-ln25\/35\/50\/60vgb-er1_firmware	2609
	msz-ln25\/35\/50\/60vgr-a1_firmware	2611
	msz-ln25\/35\/50\/60vgr-er1_firmware	2612
	msz-ln25\/35\/50\/60vgv-a1_firmware	2614
	msz-ln25\/35\/50\/60vgv-er1_firmware	2616
	msz-ln25\/35\/50\/60vgw-er1_firmware	2617
	msz-rw25\/35\/50vg-e1_firmware	2619
	msz-rw25\/35\/50vg-er1_firmware	2622
	msz-rw25\/35\/50vg-et1_firmware	2624
	msz-rw25\/35\/50vg-sc1_firmware	2627
	msz-wx18\/20\/25vfk_firmware	2630
	msz-zt09\/12\/18vak_firmware	2633
	msz-zy09\/12\/18vfk_firmware	2634
	pac-wf010-e_firmware	2637
	pac-whs01wf-e_firmware	2639
	s-mac-702if-b_firmware	2641
	s-mac-702if-f_firmware	2643
	s-mac-702if-z_firmware	2645
	s-mac-905if_firmware	2646
	s-mac-906if_firmware	2648
Oracle	solaris	2650
Phoenixcontact	fl_mguard_centerport_firmware	2651
	fl_mguard_centerport_vpn-1000_firmware	2651
	fl_mguard_core_tx_firmware	2652

Vendor	Product	Page Number
Phoenixcontact	fl_mguard_core_tx_vpn_firmware	2653
	fl_mguard_delta_tx\/tx_firmware	2653
	fl_mguard_delta_tx\/tx_vpn_firmware	2654
	fl_mguard_gt\/gt_firmware	2654
	fl_mguard_gt\/gt_vpn_firmware	2655
	fl_mguard_pci4000_firmware	2655
	fl_mguard_pci4000_vpn_firmware	2656
	fl_mguard_pcie4000_firmware	2657
	fl_mguard_pcie4000_vpn_firmware	2657
	fl_mguard_rs2000_tx\/tx-b_firmware	2658
	fl_mguard_rs2000_tx\/tx_vpn_firmware	2658
	fl_mguard_rs2005_tx_vpn_firmware	2659
	fl_mguard_rs4000_tx\/tx-m_firmware	2660
	fl_mguard_rs4000_tx\/tx-p_firmware	2660
	fl_mguard_rs4000_tx\/tx_firmware	2661
	fl_mguard_rs4000_tx\/tx_vpn_firmware	2661
	fl_mguard_rs4004_tx\/dtx_firmware	2662
	fl_mguard_rs4004_tx\/dtx_vpn_firmware	2662
	fl_mguard_smart2_firmware	2663
	fl_mguard_smart2_vpn_firmware	2664
	tc_mguard_rs2000_3g_vpn_firmware	2664
	tc_mguard_rs2000_4g_att_vpn_firmware	2665
	tc_mguard_rs2000_4g_vpn_firmware	2665
	tc_mguard_rs2000_4g_vzw_vpn_firmware	2666
	tc_mguard_rs4000_3g_vpn_firmware	2666
	tc_mguard_rs4000_4g_att_vpn_firmware	2667
	tc_mguard_rs4000_4g_vpn_firmware	2668
	tc_mguard_rs4000_4g_vzw_vpn_firmware	2668
Redhat	enterprise_linux	2669
	enterprise_linux_kernel-based_virtual_machine	2670
Samsung	exynos_firmware	2670
sick	sim1000_fx_firmware	2671

Vendor	Product	Page Number
sick	sim1004-0p0g311_firmware	2672
	sim1004_firmware	2673
	sim1012-0p0g200_firmware	2674
	sim1012_firmware	2675
	sim2000-2p04g10_firmware	2676
	sim2000st_firmware	2677
	sim2000_firmware	2679
	sim2500-2p03g10_firmware	2680
	sim2500_firmware	2680
	sim4000_firmware	2681
Siemens	6ag1151-8ab01-7ab0_firmware	2682
	6ag1151-8fb01-2ab0_firmware	2685
	6ag1314-6eh04-7ab0_firmware	2688
	6ag1315-2eh14-7ab0_firmware	2691
	6ag1315-2fj14-2ab0_firmware	2694
	6ag1317-2ek14-7ab0_firmware	2697
	6ag1317-2fk14-2ab0_firmware	2700
	6es7151-8ab01-0ab0_firmware	2703
	6es7151-8fb01-0ab0_firmware	2706
	6es7154-8ab01-0ab0_firmware	2709
	6es7154-8fb01-0ab0_firmware	2712
	6es7154-8fx00-0ab0_firmware	2715
	6es7314-6eh04-0ab0_firmware	2718
	6es7315-2eh14-0ab0_firmware	2721
	6es7315-2fj14-0ab0_firmware	2724
	6es7315-7tj10-0ab0_firmware	2727
	6es7317-2ek14-0ab0_firmware	2730
	6es7317-2fk14-0ab0_firmware	2733
	6es7317-7tk10-0ab0_firmware	2736
	6es7317-7ul10-0ab0_firmware	2739
	6es7318-3el01-0ab0_firmware	2742
	6es7318-3fl01-0ab0_firmware	2745

Vendor	Product	Page Number
Siemens	7kg9501-0aa01-2aa1_firmware	2748
	7kg9501-0aa31-2aa1_firmware	2751
	simatic_drive_controller_cpu_1504d_tf_firmware	2754
	simatic_drive_controller_cpu_1507d_tf_firmware	2757
	simatic_pcs_firmware	2760
	simatic_s7-1200_cpu_1211c_firmware	2763
	simatic_s7-1200_cpu_1212c_firmware	2766
	simatic_s7-1200_cpu_1212fc_firmware	2769
	simatic_s7-1200_cpu_1214c_firmware	2772
	simatic_s7-1200_cpu_1214fc_firmware	2775
	simatic_s7-1200_cpu_1214_fc_firmware	2778
	simatic_s7-1200_cpu_1215c_firmware	2781
	simatic_s7-1200_cpu_1215fc_firmware	2784
	simatic_s7-1200_cpu_1215_fc_firmware	2787
	simatic_s7-1200_cpu_1217c_firmware	2790
	simatic_s7-1200_cpu_12_1211c_firmware	2793
	simatic_s7-1200_cpu_12_1212c_firmware	2796
	simatic_s7-1200_cpu_12_1212fc_firmware	2799
	simatic_s7-1200_cpu_12_1214c_firmware	2802
	simatic_s7-1200_cpu_12_1214fc_firmware	2805
	simatic_s7-1200_cpu_12_1215c_firmware	2808
	simatic_s7-1200_cpu_12_1215fc_firmware	2811
	simatic_s7-1200_cpu_12_1217c_firmware	2814
	simatic_s7-1500_cpu_1507s_firmware	2817
	simatic_s7-1500_cpu_1507s_f_firmware	2820
	simatic_s7-1500_cpu_1508s_firmware	2823
	simatic_s7-1500_cpu_1508s_f_firmware	2826
	simatic_s7-1500_cpu_1510sp-1_firmware	2829
	simatic_s7-1500_cpu_1510sp_firmware	2832
	simatic_s7-1500_cpu_1511-1_firmware	2835
	simatic_s7-1500_cpu_1511-1_pn_firmware	2838

Vendor	Product	Page Number
Siemens	simatic_s7-1500_cpu_1511c-1_firmware	2841
	simatic_s7-1500_cpu_1511c_firmware	2844
	simatic_s7-1500_cpu_1511f-1_firmware	2847
	simatic_s7-1500_cpu_1511f-1_pn_firmware	2850
	simatic_s7-1500_cpu_1511t-1_firmware	2853
	simatic_s7-1500_cpu_1511tf-1_firmware	2856
	simatic_s7-1500_cpu_1512c-1_firmware	2859
	simatic_s7-1500_cpu_1512c_firmware	2862
	simatic_s7-1500_cpu_1512sp-1_firmware	2865
	simatic_s7-1500_cpu_1512spf-1_firmware	2868
	simatic_s7-1500_cpu_1513-1_firmware	2871
	simatic_s7-1500_cpu_1513-1_pn_firmware	2874
	simatic_s7-1500_cpu_1513f-1_firmware	2877
	simatic_s7-1500_cpu_1513f-1_pn_firmware	2880
	simatic_s7-1500_cpu_1513r-1_firmware	2883
	simatic_s7-1500_cpu_1515-2_firmware	2886
	simatic_s7-1500_cpu_1515-2_pn_firmware	2889
	simatic_s7-1500_cpu_151511c-1_firmware	2892
	simatic_s7-1500_cpu_151511f-1_firmware	2895
	simatic_s7-1500_cpu_1515f-2_firmware	2898
	simatic_s7-1500_cpu_1515f-2_pn_firmware	2901
	simatic_s7-1500_cpu_1515r-2_firmware	2904
	simatic_s7-1500_cpu_1515t-2_firmware	2907
	simatic_s7-1500_cpu_1515tf-2_firmware	2910
	simatic_s7-1500_cpu_1516-3_dp_firmware	2913
	simatic_s7-1500_cpu_1516-3_firmware	2916
	simatic_s7-1500_cpu_1516-3_pn\/dp_firmware	2919
	simatic_s7-1500_cpu_1516-3_pn_firmware	2922
	simatic_s7-1500_cpu_1516f-3_firmware	2925
	simatic_s7-1500_cpu_1516f-3_pn\/dp_firmware	2928
	simatic_s7-1500_cpu_1516pro-2_firmware	2931

Vendor	Product	Page Number
Siemens	simatic_s7-1500_cpu_1516pro_f_firmware	2934
	simatic_s7-1500_cpu_1516t-3_firmware	2937
	simatic_s7-1500_cpu_1516tf-3_firmware	2940
	simatic_s7-1500_cpu_1517-3_dp_firmware	2943
	simatic_s7-1500_cpu_1517-3_firmware	2946
	simatic_s7-1500_cpu_1517-3_pn\/dp_firmware	2949
	simatic_s7-1500_cpu_1517-3_pn_firmware	2952
	simatic_s7-1500_cpu_1517f-3_firmware	2955
	simatic_s7-1500_cpu_1517f-3_pn\/dp_firmware	2958
	simatic_s7-1500_cpu_1517tf-3_firmware	2961
	simatic_s7-1500_cpu_1518-4_dp_firmware	2964
	simatic_s7-1500_cpu_1518-4_firmware	2967
	simatic_s7-1500_cpu_1518-4_pn\/dp_firmware	2970
	simatic_s7-1500_cpu_1518-4_pn\/dp_mfp_firmware	2973
	simatic_s7-1500_cpu_1518-4_pn_firmware	2976
	simatic_s7-1500_cpu_1518f-4_firmware	2979
	simatic_s7-1500_cpu_1518f-4_pn\/dp_firmware	2982
	simatic_s7-1500_cpu_1518hf-4_firmware	2985
	simatic_s7-1500_cpu_1518t-4_firmware	2988
	simatic_s7-1500_cpu_1518tf-4_firmware	2991
	simatic_s7-1500_cpu_1518_firmware	2994
	simatic_s7-1500_cpu_15pro-2_firmware	2997
	simatic_s7-1500_cpu_15prof-2_firmware	3000
	simatic_s7-1500_cpu_cpu_1513pro-2_firmware	3003
	simatic_s7-1500_cpu_cpu_1513prof-2_firmware	3006
	simatic_s7-400_pn\/dp_v6_firmware	3009
	simatic_s7-400_pn\/dp_v7_firmware	3012

Vendor	Product	Page Number
Siemens	sinumerik_one_firmware	3015
Tenda	ac23_firmware	3018
westerndigital	my_cloud_home_duo_firmware	3020
	my_cloud_home_firmware	3021
	sandisk_ibi_firmware	3022
wut	at-modem-emulator_firmware	3023
	com-server_20ma_firmware	3024
	com-server_highspeed_100basefx_firmware	3025
	com-server_highspeed_100baselx_firmware	3025
	com-server_highspeed_19\"_1port_firmware	3026
	com-server_highspeed_19\"_4port_firmware	3027
	com-server_highspeed_compact_firmware	3028
	com-server_highspeed_industry_firmware	3029
	com-server_highspeed_isolated_firmware	3030
	com-server_highspeed_lc_firmware	3030
	com-server_highspeed_oem_firmware	3031
	com-server_highspeed_office_1port_firmware	3032
	com-server_highspeed_office_4port_firmware	3033
	com-server_highspeed_poe_3x_isolated_firmware	3034
	com-server_highspeed_poe_firmware	3034
	com-server_highspeed_ul_firmware	3035
	com-server_\+\+_firmware	3036
XEN	xen	3037

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 5-anker					
Product: 5_anker_connect					
Affected Version(s): * Up to (excluding) 1.2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	4.8	Auth. Reflected Cross-Site Scripting (XSS) vulnerability in 5 Anker Connect plugin <= 1.2.6 on WordPress. **CVE ID : CVE-2022-30545**	https://patchstack.com/database/vulnerability/5-anker-connect/wordpress-5-anker-connect-plugin-1-2-6-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve, https://wordpress.org/plugins/5-anker-connect/	A-5-A-5_AN-211122/1
Vendor: a3rev					
Product: page_view_count					
Affected Version(s): * Up to (including) 2.5.5					
Cross-Site Request Forgery (CSRF)	03-Nov-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in a3rev Software Page View Count plugin <= 2.5.5 on WordPress allows an attacker to reset the plugin settings. **CVE ID : CVE-2022-40131**	https://patchstack.com/database/vulnerability/page-views-count/wordpress-page-view-count-plugin-2-5-5-cross-site-request-forgery-csrf-vulnerability?_s_id=cve, https://word	A-A3R-PAGE-211122/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				press.org/plugins/page-views-count/#developers	
Vendor: Accusoft					
Product: imagegear					
Affected Version(s): 20.0					
Out-of-bounds Write	09-Nov-2022	7.8	An out-of-bounds write vulnerability exists in the PICT parsing pctwread_14841 functionality of Accusoft ImageGear 20.0. A specially-crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-32588**	N/A	A-ACC-IMAG-211122/3
Vendor: Acronis					
Product: cyber_protect_home_office					
Affected Version(s): * Up to (excluding) 39900					
Improper Privilege Management	07-Nov-2022	7.8	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 39900.	https://security-advisory.acronis.com/advisories/SEC-3040	A-ACR-CYBE-211122/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44732		
Incorrect Permission Assignment for Critical Resource	07-Nov-2022	7.8	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 39900. **CVE ID : CVE-2022-44733**	https://security-advisory.acronis.com/advisories/SEC-3968	A-ACR-CYBE-211122/5
Affected Version(s): * Up to (excluding) 40107					
Improper Link Resolution Before File Access ('Link Following')	07-Nov-2022	7.8	Local privilege escalation due to improper soft link handling. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40107. **CVE ID : CVE-2022-44747**	https://security-advisory.acronis.com/advisories/SEC-4540	A-ACR-CYBE-211122/6
Uncontrolled Search Path Element	07-Nov-2022	7.3	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40107. **CVE ID : CVE-2022-44744**	https://security-advisory.acronis.com/advisories/SEC-2718	A-ACR-CYBE-211122/7
Insertion of Sensitive	07-Nov-2022	5.5	Sensitive information leak	https://security-	A-ACR-CYBE-211122/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			through log files. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40107. **CVE ID : CVE-2022-44745**	advisory.acronis.com/advisories/SEC-3481	
Incorrect Permission Assignment for Critical Resource	07-Nov-2022	5.5	Sensitive information disclosure due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40107. **CVE ID : CVE-2022-44746**	https://security-advisory.acronis.com/advisories/SEC-4398	A-ACR-CYBE-211122/9
Vendor: activity_log_project					
Product: activity_log					
Affected Version(s): -					
Improper Encoding or Escaping of Output	11-Nov-2022	9.8	A vulnerability has been found in Activity Log Plugin and classified as critical. This vulnerability affects unknown code of the component HTTP Header Handler. The manipulation of the argument X-Forwarded-For leads to improper output neutralization for	N/A	A-ACT-ACTI-211122/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logs. 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-213448. **CVE ID : CVE-2022-3941**		
Affected Version(s): * Up to (excluding) 2.8.4					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Nov-2022	9.8	CSV Injection vulnerability in Activity Log Team Activity Log <= 2.8.3 on WordPress. **CVE ID : CVE-2022-27858**	https://wordpress.org/plugins/aryo-activity-log/#developers, https://patchstack.com/database/vulnerability/aryo-activity-log/wordpress-activity-log-plugin-2-8-3-csv-injection-vulnerability?_s_id=cve	A-ACT-ACTI-211122/11
Vendor: addify					
Product: product_stock_manager					
Affected Version(s): * Up to (excluding) 1.0.5					
Cross-Site Request Forgery (CSRF)	07-Nov-2022	4.3	The Product Stock Manager WordPress plugin before 1.0.5 does not have authorisation and proper CSRF checks in multiple AJAX actions, allowing users with a role as	https://wpscan.com/vulnerability/d8005cd0-8232-4d43-a4e4-14728eaf1300	A-ADD-PROD-211122/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			low as subscriber to call them. One action in particular could allow to update arbitrary options **CVE ID : CVE-2022-3451**		
Product: role_based_pricing_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.6.2					
Cross-Site Request Forgery (CSRF)	07-Nov-2022	8.8	The Role Based Pricing for WooCommerce WordPress plugin before 1.6.2 does not have authorisation and proper CSRF checks, and does not validate files to be uploaded, allowing any authenticated users like subscriber to upload arbitrary files, such as PHP **CVE ID : CVE-2022-3537**	https://wpscan.com/vulnerability/696868f7-409d-422d-87f4-92fc6bf6e74e	A-ADD-ROLE-211122/13
Affected Version(s): * Up to (excluding) 1.6.3					
Cross-Site Request Forgery (CSRF)	07-Nov-2022	8.8	The Role Based Pricing for WooCommerce WordPress plugin before 1.6.3 does not have authorisation and proper CSRF checks, as well as does not validate path given via user input, allowing any authenticated users	https://wpscan.com/vulnerability/6af63aab-b7a6-4ef6-8604-4b4b99467a34	A-ADD-ROLE-211122/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			like subscriber to perform PHAR deserialization attacks when they can upload a file, and a suitable gadget chain is present on the blog **CVE ID : CVE-2022-3536**		
Vendor: agenteasy_properties_project					
Product: agenteasy_properties					
Affected Version(s): * Up to (including) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in AgentEasy Properties plugin <= 1.0.4 on WordPress. **CVE ID : CVE-2022-44576**	https://wordpress.org/plugins/agenteasy-properties/, https://patchstack.com/database/vulnerability/agenteasy-properties/wordpress-agenteasy-properties-plugin-1-0-4-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve	A-AGE-AGEN-211122/15
Vendor: aioseo					
Product: all_in_one_seo					
Affected Version(s): * Up to (including) 4.2.5.1					
Server-Side Request Forgery (SSRF)	08-Nov-2022	6.5	Server Side Request Forgery (SSRF) vulnerability in All in One SEO Pro plugin <= 4.2.5.1 on WordPress.	https://aioseo.com/changelog/, https://patchstack.com/database/vulnerab	A-AIO-ALL_-211122/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42494	ility/all-in-one-seo-pack-pro/wordpress-all-in-one-seo-pro-plugin-4-2-5-1-server-side-request-forgery-ssrf-vulnerability?_s_id=cve	
Vendor: algolplus					
Product: advanced_dynamic_pricing_for_woocommerce					
Affected Version(s): * Up to (including) 4.1.5					
Cross-Site Request Forgery (CSRF)	09-Nov-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Advanced Dynamic Pricing for WooCommerce plugin <= 4.1.5 on WordPress leading to rule type migration. **CVE ID : CVE-2022-43488**	https://patchstack.com/database/vulnerability/advanced-dynamic-pricing-for-woocommerce/wordpress-advanced-dynamic-pricing-for-woocommerce-plugin-4-1-5-cross-site-request-forgery-csrf-vulnerability-2?_s_id=cve	A-ALG-ADVA-211122/17
Cross-Site Request Forgery (CSRF)	08-Nov-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Advanced Dynamic Pricing for WooCommerce plugin <= 4.1.5 on WordPress leading to plugin settings import.	https://wordpress.org/plugins/advanced-dynamic-pricing-for-woocommerce/	A-ALG-ADVA-211122/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43491		
Product: advanced_order_export					
Affected Version(s): * Up to (excluding) 3.3.3					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	6.5	Cross-Site Request Forgery (CSRF) vulnerability in Advanced Order Export For WooCommerce plugin <= 3.3.2 on WordPress leading to export file download. **CVE ID : CVE-2022-40128**	https://patchstack.com/database/vulnerability/woo-order-export-lite/wordpress-advanced-order-export-for-woocommerce-plugin-3-3-2-cross-site-request-forgery-csrf-vulnerability?_s_id=cve, https://wordpress.org/plugins/woo-order-export-lite/	A-ALG-ADVA-211122/19
Vendor: am-hili_project					
Product: am-hili					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) in Ayoub Media AM-HiLi plugin <= 1.0 on WordPress. **CVE ID : CVE-2022-44586**	https://wordpress.org/plugins/am-hili-affiliate-manager-for-publishers/, https://patchstack.com/database/vulnerability/am-hili-affiliate-manager-for-publishers/wordpress-am-	A-AM--AM-H-211122/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				hili-plugin-1-0-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve	
Vendor: Amazon					
Product: opensearch_notifications					
Affected Version(s): * Up to (excluding) 2.2.1.0					
Server-Side Request Forgery (SSRF)	11-Nov-2022	8.7	OpenSearch Notifications is a notifications plugin for OpenSearch that enables other plugins to send notifications via Email, Slack, Amazon Chime, Custom web-hook etc channels. A potential SSRF issue in OpenSearch Notifications Plugin 2.2.0 and below could allow an existing privileged user to enumerate listening services or interact with configured resources via HTTP requests exceeding the Notification plugin's intended scope. OpenSearch 2.2.1+ contains the fix for this issue. There are currently no recommended workarounds.	https://github.com/opensearch-project/notifications/pull/507, https://github.com/opensearch-project/notifications/security/advisories/GHSA-pfc4-3436-jgrw, https://github.com/opensearch-project/notifications/pull/496	A-AMA-OPEN-211122/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41906		
Vendor: AMD					
Product: amd_link					
Affected Version(s): * Up to (excluding) 5.0.220614					
N/A	09-Nov-2022	7.5	Insufficient access controls in the AMD Link Android app may potentially result in information disclosure. **CVE ID : CVE-2022-27673**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1047	A-AMD-AMD_-211122/22
Product: amd_uprof					
Affected Version(s): * Up to (excluding) 3.6.449					
N/A	09-Nov-2022	7.5	Insufficient validation of the IOCTL input buffer in AMD ?Prof may allow an attacker to send an arbitrary buffer leading to a potential Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-23831**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	A-AMD-AMD_-211122/23
N/A	09-Nov-2022	7.5	Insufficient validation in the IOCTL input/output buffer in AMD ?Prof may allow an attacker to bypass bounds checks potentially leading to a Windows kernel crash	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	A-AMD-AMD_-211122/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in denial of service. **CVE ID : CVE-2022-27674**		
Affected Version(s): * Up to (excluding) 3.6.549					
N/A	09-Nov-2022	7.5	Insufficient validation of the IOCTL input buffer in AMD ?Prof may allow an attacker to send an arbitrary buffer leading to a potential Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-23831**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	A-AMD-AMD_-211122/25
N/A	09-Nov-2022	7.5	Insufficient validation in the IOCTL input/output buffer in AMD ?Prof may allow an attacker to bypass bounds checks potentially leading to a Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-27674**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	A-AMD-AMD_-211122/26
Affected Version(s): * Up to (excluding) 3.6.839					
N/A	09-Nov-2022	7.5	Insufficient validation of the IOCTL input buffer in AMD ?Prof may allow an attacker to send an arbitrary buffer leading to a potential Windows	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	A-AMD-AMD_-211122/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel crash resulting in denial of service. **CVE ID : CVE-2022-23831**		
N/A	09-Nov-2022	7.5	Insufficient validation in the IOCTL input/output buffer in AMD ?Prof may allow an attacker to bypass bounds checks potentially leading to a Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-27674**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	A-AMD-AMD_-211122/28
Vendor: analytify					
Product: analytify_-_google_analytics_dashboard					
Affected Version(s): * Up to (excluding) 4.2.3					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Analytify plugin <= 4.2.2 on WordPress. **CVE ID : CVE-2022-38137**	https://wordpress.org/plugins/wp-analytify/, https://patchstack.com/database/vulnerability/wp-analytify/wordpress-analytify-plugin-4-2-2-cross-site-request-forgery-csrf-vulnerability?_s_id=cve	A-ANA-ANAL-211122/29
Vendor: Apache					
Product: airflow					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.3.1					
Exposure of Sensitive Information to an Unauthorized Actor	14-Nov-2022	7.5	A vulnerability in UI of Apache Airflow allows an attacker to view unmasked secrets in rendered template values for tasks which were not executed (for example when they were depending on past and previous instances of the task failed). This issue affects Apache Airflow prior to 2.3.1. **CVE ID : CVE-2022-27949**	https://github.com/apache/airflow/pull/22754, https://lists.apache.org/thread/n38oc5obb48600fsvnbopxcs0jpbp65p	A-APA-AIRF-211122/30
Affected Version(s): * Up to (excluding) 2.4.0					
Improper Control of Generation of Code ('Code Injection')	14-Nov-2022	8.8	A vulnerability in Example Dags of Apache Airflow allows an attacker with UI access who can trigger DAGs, to execute arbitrary commands via manually provided run_id parameter. This issue affects Apache Airflow Apache Airflow versions prior to 2.4.0. **CVE ID : CVE-2022-40127**	https://github.com/apache/airflow/pull/25960	A-APA-AIRF-211122/31
Affected Version(s): * Up to (excluding) 2.4.2					
Improper Neutralization of	02-Nov-2022	6.1	In Apache Airflow versions prior to 2.4.2, the "Trigger	https://lists.apache.org/thread/vqnvdrfs	A-APA-AIRF-211122/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			DAG with config" screen was susceptible to XSS attacks via the `origin` query argument. **CVE ID : CVE-2022-43982**	w9z7v7c46qh3psjgr7wy959l	
URL Redirection to Untrusted Site ('Open Redirect')	02-Nov-2022	6.1	In Apache Airflow versions prior to 2.4.2, there was an open redirect in the webserver's `/confirm` endpoint. **CVE ID : CVE-2022-43985**	https://lists.apache.org/thread/m13y9s5kw92fw9l8j4qd85h0txp4kfcq, https://github.com/apache/airflow/pull/27143	A-APA-AIRF-211122/33
Product: archiva					
Affected Version(s): * Up to (excluding) 2.2.9					
N/A	15-Nov-2022	7.5	If anonymous read enabled, it's possible to read the database file directly without logging in. **CVE ID : CVE-2022-40308**	https://lists.apache.org/thread/x01pnn0jjsw512cscxsbxzrjmz64n4cc	A-APA-ARCH-211122/34
N/A	15-Nov-2022	4.3	Users with write permissions to a repository can delete arbitrary directories. **CVE ID : CVE-2022-40309**	https://lists.apache.org/thread/1odl4p85r96n27k577jk6ftrp19xfc27	A-APA-ARCH-211122/35
Product: commons_bcel					
Affected Version(s): * Up to (excluding) 6.6.0					
Out-of-bounds Write	07-Nov-2022	9.8	Apache Commons BCEL has a number of APIs that would	https://lists.apache.org/thread/lfxk7q8q	A-APA-COMM-211122/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			normally only allow changing specific class characteristics. However, due to an out-of-bounds writing issue, these APIs can be used to produce arbitrary bytecode. This could be abused in applications that pass attacker-controllable data to those APIs, giving the attacker more control over the resulting bytecode than otherwise expected. Update to Apache Commons BCEL 6.6.0. **CVE ID : CVE-2022-42920**	mnh5bt9jm6nmjlv5hsxjhrz4	
Product: dolphinscheduler					
Affected Version(s): * Up to (excluding) 3.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Nov-2022	6.5	When users add resources to the resource center with a relation path will cause path traversal issues and only for logged-in users. You could upgrade to version 3.0.0 or higher **CVE ID : CVE-2022-34662**	N/A	A-APA-DOLP-211122/37
Product: ivy					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.5.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Nov-2022	7.5	When Apache Ivy downloads artifacts from a repository it stores them in the local file system based on a user-supplied "pattern" that may include placeholders for artifacts coordinates like the organisation, module or version. If said coordinates contain "../" sequences - which are valid characters for Ivy coordinates in general - it is possible the artifacts are stored outside of Ivy's local cache or repository or can overwrite different artifacts inside of the local cache. In order to exploit this vulnerability an attacker needs collaboration by the remote repository as Ivy will issue http requests containing ".." sequences and a "normal" repository will not interpret them as part of the artifact coordinates. Users of Apache Ivy 2.0.0 to 2.5.1 should	https://lists.apache.org/thread/htxbr8oc464hxrgroftnz3my70whk93b	A-APA-IVY-211122/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to Ivy 2.5.1. **CVE ID : CVE-2022-37866**		
Affected Version(s): From (including) 2.4.0 Up to (excluding) 2.5.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Nov-2022	9.1	With Apache Ivy 2.4.0 an optional packaging attribute has been introduced that allows artifacts to be unpacked on the fly if they used pack200 or zip packaging. For artifacts using the "zip", "jar" or "war" packaging Ivy prior to 2.5.1 doesn't verify the target path when extracting the archive. An archive containing absolute paths or paths that try to traverse "upwards" using ".." sequences can then write files to any location on the local fie system that the user executing Ivy has write access to. Ivy users of version 2.4.0 to 2.5.0 should upgrade to Ivy 2.5.1. **CVE ID : CVE-2022-37865**	https://lists.apache.org/thread/gqvvv7qsm2dfjg6xzsw1s2h08tbr0sdy	A-APA-IVY-211122/39
Product: pulsar					
Affected Version(s): * Up to (including) 2.6.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	04-Nov-2022	8.1	The Apache Pulsar C++ Client does not verify peer TLS certificates when making HTTPS calls for the OAuth2.0 Client Credential Flow, even when tlsAllowInsecureConnection is disabled via configuration. This vulnerability allows an attacker to perform a man in the middle attack and intercept and/or modify the GET request that is sent to the ClientCredentialFlow 'issuer url'. The intercepted credentials can be used to acquire authentication data from the OAuth2.0 server to then authenticate with an Apache Pulsar cluster. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. The Apache Pulsar Python Client wraps the C++ client, so it is	https://lists.apache.org/thread/ky1ssskvkj00y36k7nys9b5gm5jjrzwv	A-APA-PULS-211122/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also vulnerable in the same way. This issue affects Apache Pulsar C++ Client and Python Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0 to 2.10.1; 2.6.4 and earlier. Any users running affected versions of the C++ Client or the Python Client should rotate vulnerable OAuth2.0 credentials, including client_id and client_secret. 2.7 C++ and Python Client users should upgrade to 2.7.5 and rotate vulnerable OAuth2.0 credentials. 2.8 C++ and Python Client users should upgrade to 2.8.4 and rotate vulnerable OAuth2.0 credentials. 2.9 C++ and Python Client users should upgrade to 2.9.3 and rotate vulnerable OAuth2.0 credentials. 2.10 C++ and Python Client users should upgrade to 2.10.2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and rotate vulnerable OAuth2.0 credentials. 3.0 C++ users are unaffected and 3.0 Python Client users will be unaffected when it is released. Any users running the C++ and Python Client for 2.6 or less should upgrade to one of the above patched versions. **CVE ID : CVE-2022-33684**		
Affected Version(s): From (including) 2.10.0 Up to (excluding) 2.10.2					
Improper Certificate Validation	04-Nov-2022	8.1	The Apache Pulsar C++ Client does not verify peer TLS certificates when making HTTPS calls for the OAuth2.0 Client Credential Flow, even when tlsAllowInsecureConnection is disabled via configuration. This vulnerability allows an attacker to perform a man in the middle attack and intercept and/or modify the GET request that is sent to the ClientCredentialFlow 'issuer url'. The intercepted credentials can be used to acquire authentication data	https://lists.apache.org/thread/ky1ssskvkj00y36k7nys9b5gm5jjrzwv	A-APA-PULS-211122/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the OAuth2.0 server to then authenticate with an Apache Pulsar cluster. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. The Apache Pulsar Python Client wraps the C++ client, so it is also vulnerable in the same way. This issue affects Apache Pulsar C++ Client and Python Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0 to 2.10.1; 2.6.4 and earlier. Any users running affected versions of the C++ Client or the Python Client should rotate vulnerable OAuth2.0 credentials, including client_id and client_secret. 2.7 C++ and Python Client users should upgrade to 2.7.5 and rotate vulnerable		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OAuth2.0 credentials. 2.8 C++ and Python Client users should upgrade to 2.8.4 and rotate vulnerable OAuth2.0 credentials. 2.9 C++ and Python Client users should upgrade to 2.9.3 and rotate vulnerable OAuth2.0 credentials. 2.10 C++ and Python Client users should upgrade to 2.10.2 and rotate vulnerable OAuth2.0 credentials. 3.0 C++ users are unaffected and 3.0 Python Client users will be unaffected when it is released. Any users running the C++ and Python Client for 2.6 or less should upgrade to one of the above patched versions. **CVE ID : CVE-2022-33684**		
Affected Version(s): From (including) 2.7.0 Up to (excluding) 2.7.5					
Improper Certificate Validation	04-Nov-2022	8.1	The Apache Pulsar C++ Client does not verify peer TLS certificates when making HTTPS calls for the OAuth2.0	https://lists.apache.org/thread/ky1ssskvkj00y36k7nys9b5gm5jjrzwv	A-APA-PULS-211122/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Client Credential Flow, even when tlsAllowInsecureConnection is disabled via configuration. This vulnerability allows an attacker to perform a man in the middle attack and intercept and/or modify the GET request that is sent to the ClientCredentialFlow 'issuer url'. The intercepted credentials can be used to acquire authentication data from the OAuth2.0 server to then authenticate with an Apache Pulsar cluster. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. The Apache Pulsar Python Client wraps the C++ client, so it is also vulnerable in the same way. This issue affects Apache Pulsar C++ Client and Python Client versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0 to 2.10.1; 2.6.4 and earlier. Any users running affected versions of the C++ Client or the Python Client should rotate vulnerable OAuth2.0 credentials, including client_id and client_secret. 2.7 C++ and Python Client users should upgrade to 2.7.5 and rotate vulnerable OAuth2.0 credentials. 2.8 C++ and Python Client users should upgrade to 2.8.4 and rotate vulnerable OAuth2.0 credentials. 2.9 C++ and Python Client users should upgrade to 2.9.3 and rotate vulnerable OAuth2.0 credentials. 2.10 C++ and Python Client users should upgrade to 2.10.2 and rotate vulnerable OAuth2.0 credentials. 3.0 C++ users are unaffected and 3.0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Python Client users will be unaffected when it is released. Any users running the C++ and Python Client for 2.6 or less should upgrade to one of the above patched versions. **CVE ID : CVE-2022-33684**		
Affected Version(s): From (including) 2.8.0 Up to (excluding) 2.8.4					
Improper Certificate Validation	04-Nov-2022	8.1	The Apache Pulsar C++ Client does not verify peer TLS certificates when making HTTPS calls for the OAuth2.0 Client Credential Flow, even when tlsAllowInsecureConnection is disabled via configuration. This vulnerability allows an attacker to perform a man in the middle attack and intercept and/or modify the GET request that is sent to the ClientCredentialFlow 'issuer url'. The intercepted credentials can be used to acquire authentication data from the OAuth2.0 server to then authenticate with an Apache Pulsar cluster. An attacker can only take	https://lists.apache.org/thread/ky1ssskvkj00y36k7nys9b5gm5jjrzwv	A-APA-PULS-211122/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. The Apache Pulsar Python Client wraps the C++ client, so it is also vulnerable in the same way. This issue affects Apache Pulsar C++ Client and Python Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0 to 2.10.1; 2.6.4 and earlier. Any users running affected versions of the C++ Client or the Python Client should rotate vulnerable OAuth2.0 credentials, including client_id and client_secret. 2.7 C++ and Python Client users should upgrade to 2.7.5 and rotate vulnerable OAuth2.0 credentials. 2.8 C++ and Python Client users should upgrade to 2.8.4 and rotate		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable OAuth2.0 credentials. 2.9 C++ and Python Client users should upgrade to 2.9.3 and rotate vulnerable OAuth2.0 credentials. 2.10 C++ and Python Client users should upgrade to 2.10.2 and rotate vulnerable OAuth2.0 credentials. 3.0 C++ users are unaffected and 3.0 Python Client users will be unaffected when it is released. Any users running the C++ and Python Client for 2.6 or less should upgrade to one of the above patched versions. **CVE ID : CVE-2022-33684**		
Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.3					
Improper Certificate Validation	04-Nov-2022	8.1	The Apache Pulsar C++ Client does not verify peer TLS certificates when making HTTPS calls for the OAuth2.0 Client Credential Flow, even when tlsAllowInsecureConnection is disabled via configuration. This vulnerability	https://lists.apache.org/thread/ky1ssskvkj00y36k7nys9b5gm5jjrzwv	A-APA-PULS-211122/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an attacker to perform a man in the middle attack and intercept and/or modify the GET request that is sent to the ClientCredentialFlow 'issuer url'. The intercepted credentials can be used to acquire authentication data from the OAuth2.0 server to then authenticate with an Apache Pulsar cluster. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. The Apache Pulsar Python Client wraps the C++ client, so it is also vulnerable in the same way. This issue affects Apache Pulsar C++ Client and Python Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0 to 2.10.1; 2.6.4 and earlier. Any users running affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions of the C++ Client or the Python Client should rotate vulnerable OAuth2.0 credentials, including client_id and client_secret. 2.7 C++ and Python Client users should upgrade to 2.7.5 and rotate vulnerable OAuth2.0 credentials. 2.8 C++ and Python Client users should upgrade to 2.8.4 and rotate vulnerable OAuth2.0 credentials. 2.9 C++ and Python Client users should upgrade to 2.9.3 and rotate vulnerable OAuth2.0 credentials. 2.10 C++ and Python Client users should upgrade to 2.10.2 and rotate vulnerable OAuth2.0 credentials. 3.0 C++ users are unaffected and 3.0 Python Client users will be unaffected when it is released. Any users running the C++ and Python Client for 2.6 or less		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should upgrade to one of the above patched versions. **CVE ID : CVE-2022-33684**		
Product: sling_cms					
Affected Version(s): * Up to (including) 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation ('Cross-site Scripting') [CWE-79] vulnerability in Sling App CMS version 1.1.0 and prior may allow an authenticated remote attacker to perform a reflected cross site scripting (XSS) attack in the taxonomy management feature. **CVE ID : CVE-2022-43670**	https://lists.apache.org/thread/o68l3l3crfxz107fr9dm74y8vg8kj2cs	A-APA-SLIN-211122/45
Product: soap					
Affected Version(s): * Up to (including) 2.3					
Improper Authentication	14-Nov-2022	9.8	** UNSUPPORTED WHEN ASSIGNED ** In the default configuration of Apache SOAP, an RPCRouterServlet is available without authentication. This gives an attacker the possibility to invoke methods on the classpath that	https://lists.apache.org/thread/g4l64s283njhnph2otx7q4gs2j952d31	A-APA-SOAP-211122/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			meet certain criteria. Depending on what classes are available on the classpath this might even lead to arbitrary remote code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2022-45378**		
Product: spark					
Affected Version(s): * Up to (excluding) 3.2.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Nov-2022	5.4	A stored cross-site scripting (XSS) vulnerability in Apache Spark 3.2.1 and earlier, and 3.3.0, allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the logs which would be returned in logs rendered in the UI. **CVE ID : CVE-2022-31777**	N/A	A-APA-SPAR-211122/47
Affected Version(s): 3.3.0					
Improper Neutralization of Special Elements	01-Nov-2022	5.4	A stored cross-site scripting (XSS) vulnerability in Apache Spark 3.2.1 and earlier, and	N/A	A-APA-SPAR-211122/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in Output Used by a Downstream Component ('Injection')			3.3.0, allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the logs which would be returned in logs rendered in the UI. **CVE ID : CVE-2022-31777**		
Product: tomcat					
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.27					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	01-Nov-2022	7.5	If Apache Tomcat 8.5.0 to 8.5.52, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.	https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq	A-APA-TOMC-211122/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42252		
Affected Version(s): From (including) 10.1.0 Up to (excluding) 10.1.1					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	01-Nov-2022	7.5	If Apache Tomcat 8.5.0 to 8.5.52, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header. **CVE ID : CVE-2022-42252**	https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq	A-APA-TOMC-211122/50
Affected Version(s): From (including) 8.5.0 Up to (including) 8.5.52					
Inconsistent Interpretation of HTTP Requests ('HTTP Request	01-Nov-2022	7.5	If Apache Tomcat 8.5.0 to 8.5.52, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via	https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq	A-APA-TOMC-211122/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Smuggling')			setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header. **CVE ID : CVE-2022-42252**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.68					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	01-Nov-2022	7.5	If Apache Tomcat 8.5.0 to 8.5.52, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind	https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq	A-APA-TOMC-211122/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a reverse proxy that also failed to reject the request with the invalid header. **CVE ID : CVE-2022-42252**		
Product: unstructured_information_management_architecture					
Affected Version(s): * Up to (including) 3.3.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Nov-2022	7.5	A relative path traversal vulnerability in a FileUtil class used by the PEAR management component of Apache UIMA allows an attacker to create files outside the designated target directory using carefully crafted ZIP entry names. This issue affects Apache UIMA Apache UIMA version 3.3.0 and prior versions. Note that PEAR files should never be installed into an UIMA installation from untrusted sources because PEAR archives are executable plugins that will be able to perform any actions with the same privileges as	https://lists.apache.org/thread/57vk0d79j94d0lk0vol8xn935yv1shdd	A-APA-UNST-211122/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the host Java Virtual Machine. **CVE ID : CVE-2022-32287**		
Vendor: Apereo					
Product: phpcas					
Affected Version(s): * Up to (excluding) 1.6.0					
N/A	01-Nov-2022	8	phpCAS is an authentication library that allows PHP applications to easily authenticate users via a Central Authentication Service (CAS) server. The phpCAS library uses HTTP headers to determine the service URL used to validate tickets. This allows an attacker to control the host header and use a valid ticket granted for any authorized service in the same SSO realm (CAS server) to authenticate to the service protected by phpCAS. Depending on the settings of the CAS server service registry in worst case this may be any other service URL (if the allowed URLs are configured to "^(https)://.*") or	https://github.com/apereo/phpCAS/security/advisories/GHSA-8q72-6qq8-xv64	A-APE-PHPC-211122/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be strictly limited to known and authorized services in the same SSO federation if proper URL service validation is applied. This vulnerability may allow an attacker to gain access to a victim's account on a vulnerable CASified service without victim's knowledge, when the victim visits attacker's website while being logged in to the same CAS server. phpCAS 1.6.0 is a major version upgrade that starts enforcing service URL discovery validation, because there is unfortunately no 100% safe default config to use in PHP. Starting this version, it is required to pass in an additional service base URL argument when constructing the client class. For more information, please refer to the upgrading doc. This vulnerability only		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts the CAS client that the phpCAS library protects against. The problematic service URL discovery behavior in phpCAS < 1.6.0 will only be disabled, and thus you are not impacted from it, if the phpCAS configuration has the following setup: 1. `phpCAS::setUrl()` is called (a reminder that you have to pass in the full URL of the current page, rather than your service base URL), and 2. `phpCAS::setCallbackURL()` is called, only when the proxy mode is enabled. 3. If your PHP's HTTP header input `X-Forwarded-Host`, `X-Forwarded-Server`, `Host`, `X-Forwarded-Proto`, `X-Forwarded-Protocol` is sanitized before reaching PHP (by a reverse proxy, for example), you will not be impacted by this vulnerability		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either. If your CAS server service registry is configured to only allow known and trusted service URLs the severity of the vulnerability is reduced substantially in its severity since an attacker must be in control of another authorized service. Otherwise, you should upgrade the library to get the safe service discovery behavior. **CVE ID : CVE-2022-39369**		
Vendor: Apple					
Product: itunes					
Affected Version(s): * Up to (excluding) 12.12.4					
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5, iTunes 12.12.4 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-	A-APP-ITUN-211122/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26717	us/HT213260, https://support.apple.com/en-us/HT213258, https://support.apple.com/en-us/HT213259	
Product: safari					
Affected Version(s): * Up to (excluding) 15.5					
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26709**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	A-APP-SAFA-211122/56
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in	https://support.apple.com/en-us/HT213257, https://suppo	A-APP-SAFA-211122/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26716**	rt.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5, iTunes 12.12.4 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26717**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258, https://suppo	A-APP-SAFA-211122/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rt.apple.com/en-us/HT213259	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26719**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	A-APP-SAFA-211122/59
Affected Version(s): * Up to (excluding) 16.0					
N/A	01-Nov-2022	8.6	An access issue was addressed with improvements to the sandbox. This issue is fixed in Safari 16, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13. A sandboxed process may be able to circumvent sandbox restrictions.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445,	A-APP-SAFA-211122/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32892	https://support.apple.com/en-us/HT213446	
Affected Version(s): * Up to (excluding) 16.1					
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32922**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213489	A-APP-SAFA-211122/61
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-42823**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/	A-APP-SAFA-211122/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213489	
N/A	01-Nov-2022	6.5	A correctness issue in the JIT was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose internal states of the app. **CVE ID : CVE-2022-32923**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	A-APP-SAFA-211122/63
Improper Restriction of Rendered UI Layers or Frames	01-Nov-2022	6.1	The issue was addressed with improved UI handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Visiting a malicious website	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/	A-APP-SAFA-211122/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to user interface spoofing. **CVE ID : CVE-2022-42799**	en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state management. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose sensitive user information. **CVE ID : CVE-2022-42824**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	A-APP-SAFA-211122/65
Vendor: archesproject					
Product: arches					
Affected Version(s): * Up to (including) 6.1.1					
Improper Neutralization of	11-Nov-2022	9.8	Arches is a web platform for creating, managing,	https://github.com/archesproject/arches	A-ARC-ARCH-211122/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			& visualizing geospatial data. Versions prior to 6.1.2, 6.2.1, and 7.1.2 are vulnerable to SQL Injection. With a carefully crafted web request, it's possible to execute certain unwanted sql statements against the database. This issue is fixed in version 7.12, 6.2.1, and 6.1.2. Users are recommended to upgrade as soon as possible. There are no workarounds. **CVE ID : CVE-2022-41892**	/security/advisories/GHSA-gmpq-xrxj-xh8m	
Affected Version(s): 6.2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Nov-2022	9.8	Arches is a web platform for creating, managing, & visualizing geospatial data. Versions prior to 6.1.2, 6.2.1, and 7.1.2 are vulnerable to SQL Injection. With a carefully crafted web request, it's possible to execute certain unwanted sql statements against the database. This issue is fixed in version 7.12, 6.2.1, and	https://github.com/archesproject/arches/security/advisories/GHSA-gmpq-xrxj-xh8m	A-ARC-ARCH-211122/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.1.2. Users are recommended to upgrade as soon as possible. There are no workarounds. **CVE ID : CVE-2022-41892**		
Affected Version(s): 7.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Nov-2022	9.8	Arches is a web platform for creating, managing, & visualizing geospatial data. Versions prior to 6.1.2, 6.2.1, and 7.1.2 are vulnerable to SQL Injection. With a carefully crafted web request, it's possible to execute certain unwanted sql statements against the database. This issue is fixed in version 7.12, 6.2.1, and 6.1.2. Users are recommended to upgrade as soon as possible. There are no workarounds. **CVE ID : CVE-2022-41892**	https://github.com/archesproject/arches/security/advisories/GHSA-gmpq-xrxj-xh8m	A-ARC-ARCH-211122/68
Affected Version(s): 7.1.0					
Improper Neutralization of Special Elements used in an SQL	11-Nov-2022	9.8	Arches is a web platform for creating, managing, & visualizing geospatial data. Versions prior to 6.1.2, 6.2.1, and	https://github.com/archesproject/arches/security/advisories/GHSA-gmpq-xrxj-xh8m	A-ARC-ARCH-211122/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			7.1.2 are vulnerable to SQL Injection. With a carefully crafted web request, it's possible to execute certain unwanted sql statements against the database. This issue is fixed in version 7.12, 6.2.1, and 6.1.2. Users are recommended to upgrade as soon as possible. There are no workarounds. **CVE ID : CVE-2022-41892**		
Affected Version(s): 7.1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Nov-2022	9.8	Arches is a web platform for creating, managing, & visualizing geospatial data. Versions prior to 6.1.2, 6.2.1, and 7.1.2 are vulnerable to SQL Injection. With a carefully crafted web request, it's possible to execute certain unwanted sql statements against the database. This issue is fixed in version 7.12, 6.2.1, and 6.1.2. Users are recommended to upgrade as soon as	https://github.com/archesproject/arches/security/advisories/GHSA-gmpq-xrxj-xh8m	A-ARC-ARCH-211122/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible. There are no workarounds. **CVE ID : CVE-2022-41892**		
Vendor: ARM					
Product: valhall_gpu_kernel_driver					
Affected Version(s): From (including) r29p0 Up to (excluding) r38p2					
N/A	08-Nov-2022	8.8	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to obtain write access to read-only memory, or obtain access to already freed memory. This affects Valhall r29p0 through r38p1 before r38p2, and r39p0 before r40p0. **CVE ID : CVE-2022-41757**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-VALH-211122/71
Affected Version(s): r39p0					
N/A	08-Nov-2022	8.8	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to obtain write access to read-only memory, or obtain access to already freed memory. This	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-VALH-211122/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Valhall r29p0 through r38p1 before r38p2, and r39p0 before r40p0. **CVE ID : CVE-2022-41757**		
Vendor: Atlassian					
Product: confluence_data_center					
Affected Version(s): * Up to (excluding) 1.3.5					
Exposure of Sensitive Information to an Unauthorized Actor	15-Nov-2022	7.5	The Netic User Export add-on before 1.3.5 for Atlassian Confluence has the functionality to generate a list of users in the application, and export it. During export, the HTTP request has a fileName parameter that accepts any file on the system (e.g., an SSH private key) to be downloaded. **CVE ID : CVE-2022-42977**	N/A	A-ATL-CONF-211122/73
Incorrect Authorization	15-Nov-2022	7.5	In the Netic User Export add-on before 1.3.5 for Atlassian Confluence, authorization is mishandled. An unauthenticated attacker could access files on the remote system.	N/A	A-ATL-CONF-211122/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42978		
Vendor: auieo					
Product: candidats					
Affected Version(s): 3.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Nov-2022	9.8	CandidATS version 3.0.0 allows an external attacker to perform CRUD operations on the application databases. This is possible because the application does not correctly validate the entriesPerPage parameter against SQLi attacks. **CVE ID : CVE-2022-42744**	N/A	A-AUI-CAND-211122/75
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	8.8	CandidATS version 3.0.0 allows an external attacker to steal the cookie of arbitrary users. This is possible because the application does not correctly validate the files uploaded by the user. **CVE ID : CVE-2022-42750**	N/A	A-AUI-CAND-211122/76
Cross-Site Request Forgery (CSRF)	03-Nov-2022	8.8	CandidATS version 3.0.0 allows an external attacker to elevate privileges in the application. This is possible	N/A	A-AUI-CAND-211122/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the application suffers from CSRF. This allows to persuade an administrator to create a new account with administrative permissions. **CVE ID : CVE-2022-42751**		
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	03-Nov-2022	7.5	CandidATS version 3.0.0 allows an external attacker to read arbitrary files from the server. This is possible because the application is vulnerable to XXE. **CVE ID : CVE-2022-42745**	N/A	A-AUI-CAND-211122/78
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	6.1	CandidATS version 3.0.0 on 'indexFile' of the 'ajax.php' resource, allows an external attacker to steal the cookie of arbitrary users. This is possible because the application application does not properly validate user input against XSS attacks. **CVE ID : CVE-2022-42746**	N/A	A-AUI-CAND-211122/79
Improper Neutralization of Input	03-Nov-2022	6.1	CandidATS version 3.0.0 on 'sortBy' of the 'ajax.php' resource, allows an	N/A	A-AUI-CAND-211122/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			external attacker to steal the cookie of arbitrary users. This is possible because the application application does not properly validate user input against XSS attacks. **CVE ID : CVE-2022-42747**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	6.1	CandidATS version 3.0.0 on 'sortDirection' of the 'ajax.php' resource, allows an external attacker to steal the cookie of arbitrary users. This is possible because the application application does not properly validate user input against XSS attacks. **CVE ID : CVE-2022-42748**	N/A	A-AUI-CAND-211122/81
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	6.1	CandidATS version 3.0.0 on 'page' of the 'ajax.php' resource, allows an external attacker to steal the cookie of arbitrary users. This is possible because the application application does not properly	N/A	A-AUI-CAND-211122/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate user input against XSS attacks. **CVE ID : CVE-2022-42749**		
Vendor: axiosys					
Product: bento4					
Affected Version(s): -					
Improper Resource Shutdown or Release	01-Nov-2022	6.5	A vulnerability was found in Axiomatic Bento4. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Incomplete Fix CVE-2019-13238. The manipulation leads to resource consumption. 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-212660. **CVE ID : CVE-2022-3807**	N/A	A-AXI-BENT-211122/83
Affected Version(s): * Up to (including) 1.6.0-639					
Improper Resource Shutdown or Release	02-Nov-2022	6.5	A vulnerability was found in Axiomatic Bento4 and classified as problematic. Affected by this issue is the function	N/A	A-AXI-BENT-211122/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ParseCommandLine of the file Mp4Tag/Mp4Tag.cpp of the component mp4tag. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-212666 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3809**		
Improper Resource Shutdown or Release	02-Nov-2022	6.5	A vulnerability was found in Axiomatic Bento4. It has been classified as problematic. This affects the function AP4_File::AP4_File of the file Mp42Hevc.cpp of the component mp42hevc. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212667.	https://vuldb.com/?id.212667	A-AXI-BENT-211122/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3810		
Affected Version(s): 1.6.0-639					
Improper Resource Shutdown or Release	01-Nov-2022	6.5	A vulnerability was found in Axiomatic Bento4. It has been rated as problematic. Affected by this issue is the function AP4_ContainerAtom::AP4_ContainerAtom of the component mp4encrypt. The manipulation leads to memory leak. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-212678 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3812**	N/A	A-AXI-BENT-211122/86
Improper Resource Shutdown or Release	01-Nov-2022	6.5	A vulnerability classified as problematic has been found in Axiomatic Bento4. This affects an unknown part of the component mp4edit. The manipulation leads to memory leak. It is possible to initiate the attack remotely. The	N/A	A-AXI-BENT-211122/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212679. **CVE ID : CVE-2022-3813**		
Improper Resource Shutdown or Release	01-Nov-2022	6.5	A vulnerability classified as problematic was found in Axiomatic Bento4. This vulnerability affects unknown code of the component mp4decrypt. The manipulation leads to memory leak. 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-212680. **CVE ID : CVE-2022-3814**	N/A	A-AXI-BENT-211122/88
Improper Resource Shutdown or Release	01-Nov-2022	6.5	A vulnerability, which was classified as problematic, has been found in Axiomatic Bento4. This issue affects some unknown processing of the component mp4decrypt. The	N/A	A-AXI-BENT-211122/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to memory leak. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212681 was assigned to this vulnerability. **CVE ID : CVE-2022-3815**		
Improper Resource Shutdown or Release	01-Nov-2022	6.5	A vulnerability, which was classified as problematic, was found in Axiomatic Bento4. Affected is an unknown function of the component mp4decrypt. The manipulation leads to memory leak. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-212682 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3816**	N/A	A-AXI-BENT-211122/90
Improper Resource Shutdown or Release	01-Nov-2022	6.5	A vulnerability has been found in Axiomatic Bento4 and classified as problematic.	N/A	A-AXI-BENT-211122/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected by this vulnerability is an unknown functionality of the component mp4mux. The manipulation leads to memory leak. 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-212683. **CVE ID : CVE-2022-3817**		
Vendor: ayacms_project					
Product: ayacms					
Affected Version(s): 3.1.2					
Unrestricted Upload of File with Dangerous Type	10-Nov-2022	9.8	AyaCMS v3.1.2 was discovered to contain an arbitrary file upload vulnerability via the component /admin/fst_upload.inc.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-43074**	N/A	A-AYA-AYAC-211122/92
Vendor: Bitdefender					
Product: engines					
Affected Version(s): * Up to (excluding) 7.92659					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	01-Nov-2022	5.5	An Improper Access Control vulnerability in the bdservicehost.exe component, as used in Bitdefender Engines for Windows, allows an attacker to delete privileged registry keys by pointing a Registry symlink to a privileged key. This issue affects: Bitdefender Engines versions prior to 7.92659. It also affects Bitdefender Antivirus Free, Bitdefender Antivirus Plus, Bitdefender Internet Security, Bitdefender Total Security, as well as Bitdefender Endpoint Security Tools for Windows with engine versions prior to 7.92659. **CVE ID : CVE-2022-3369**	https://www.bitdefender.com/support/security-advisories/improper-handling-of-registry-symbolic-links-in-bitdefender-engines-va-10562	A-BIT-ENGI-211122/93
Vendor: bluecoral					
Product: chat_bubble					
Affected Version(s): * Up to (excluding) 2.3					
Improper Neutralization of Input During	14-Nov-2022	6.1	The Chat Bubble WordPress plugin before 2.3 does not sanitise and escape some contact	https://wpscan.com/vulnerability/012c5b64-ef76-	A-BLU-CHAT-211122/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			parameters, which could allow unauthenticated attackers to set Stored Cross-Site Scripting payloads in them, which will trigger when an admin view the related contact message **CVE ID : CVE-2022-3415**	4539-afd8-40f6c329ae88	
Vendor: BMC					
Product: remedy_it_service_management_suite					
Affected Version(s): 20.02					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	An issue was discovered in BMC Remedy before 22.1. Email-based Incident Forwarding allows remote authenticated users to inject HTML (such as an SSRF payload) into the Activity Log by placing it in the To: field. This affects rendering that occurs upon a click in the "number of recipients" field. NOTE: the vendor's position is that "no real impact is demonstrated." **CVE ID : CVE-2022-26088**	N/A	A-BMC-REME-211122/95
Vendor: bruhn-newtech					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cbrn-analysis					
Affected Version(s): * Up to (excluding) 22					
Incorrect Permission Assignment for Critical Resource	12-Nov-2022	8.8	CBRN-Analysis before 22 has weak file permissions under Public Profile, leading to disclosure of file contents or privilege escalation. **CVE ID : CVE-2022-45193**	N/A	A-BRU-CBRN-211122/96
Improper Restriction of XML External Entity Reference	12-Nov-2022	4.7	CBRN-Analysis before 22 allows XXE attacks via am mws XML document, leading to NTLMv2-SSP hash disclosure. **CVE ID : CVE-2022-45194**	N/A	A-BRU-CBRN-211122/97
Vendor: btcd_project					
Product: btcd					
Affected Version(s): * Up to (excluding) 0.23.2					
N/A	07-Nov-2022	9.8	btcd before 0.23.2, as used in Lightning Labs lnd before 0.15.2-beta and other Bitcoin-related products, mishandles witness size checking. **CVE ID : CVE-2022-44797**	https://github.com/btcsuite/btcd/pull/1896	A-BTC-BTCD-211122/98
Vendor: bytecodealliance					
Product: wasmtime					
Affected Version(s): * Up to (excluding) 1.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Nov-2022	9.8	Wasmtime is a standalone runtime for WebAssembly. Prior to version 2.0.2, there is a bug in Wasmtime's C API implementation where the definition of the `wasmtime_trap_code` does not match its declared signature in the `wasmtime/trap.h` header file. This discrepancy causes the function implementation to perform a 4-byte write into a 1-byte buffer provided by the caller. This can lead to three zero bytes being written beyond the 1-byte location provided by the caller. This bug has been patched and users should upgrade to Wasmtime 2.0.2. This bug can be worked around by providing a 4-byte buffer casted to a 1-byte buffer when calling `wasmtime_trap_code`. Users of the `wasmtime` crate are not affected by this issue, only users of the C API	https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-h84q-m8rr-3v9q, https://github.com/bytecodealliance/wasmtime/commit/087d9d7becf7422b3f872a3bcd5d97bb7ce7ff36	A-BYT-WASM-211122/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function `wasmtime_trap_code` are affected. **CVE ID : CVE-2022-39394**		
Out-of-bounds Write	10-Nov-2022	7.4	Wasmtime is a standalone runtime for WebAssembly. Prior to version 2.0.2, there is a bug in Wasmtime's implementation of its pooling instance allocator when the allocator is configured to give WebAssembly instances a maximum of zero pages of memory. In this configuration, the virtual memory mapping for WebAssembly memories did not meet the compiler-required configuration requirements for safely executing WebAssembly modules. Wasmtime's default settings require virtual memory page faults to indicate that wasm reads/writes are out-of-bounds, but the pooling allocator's configuration	https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-44mr-8vmm-wjhg, https://github.com/bytecodealliance/wasmtime/commit/e60c3742904ccbb3e26da201c9221c38a4981d72	A-BYT-WASM-211122/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would not create an appropriate virtual memory mapping for this meaning out of bounds reads/writes can successfully read/write memory unrelated to the wasm sandbox within range of the base address of the memory mapping created by the pooling allocator. This bug is not applicable with the default settings of the `wasmtime` crate. This bug can only be triggered by setting `InstanceLimits::memory_pages` to zero. This is expected to be a very rare configuration since this means that wasm modules cannot allocate any pages of linear memory. All wasm modules produced by all current toolchains are highly likely to use linear memory, so it's expected to be unlikely that this configuration is set to zero by any production embedding of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wasmtime. This bug has been patched and users should upgrade to Wasmtime 2.0.2. This bug can be worked around by increasing the `memory_pages` allotment when configuring the pooling allocator to a value greater than zero. If an embedding wishes to still prevent memory from actually being used then the `Store::limiter` method can be used to dynamically disallow growth of memory beyond 0 bytes large. Note that the default `memory_pages` value is greater than zero. **CVE ID : CVE-2022-39392**		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.2					
Out-of-bounds Write	10-Nov-2022	9.8	Wasmtime is a standalone runtime for WebAssembly. Prior to version 2.0.2, there is a bug in Wasmtime's C API implementation where the definition of the `wasmtime_trap_co	https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-h84q-m8rr-3v9q, https://github.com/bytecodealliance/wasmtime/commi	A-BYT-WASM-211122/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			de` does not match its declared signature in the `wasmtime/trap.h` header file. This discrepancy causes the function implementation to perform a 4-byte write into a 1-byte buffer provided by the caller. This can lead to three zero bytes being written beyond the 1-byte location provided by the caller. This bug has been patched and users should upgrade to Wasmtime 2.0.2. This bug can be worked around by providing a 4-byte buffer casted to a 1-byte buffer when calling `wasmtime_trap_code`. Users of the `wasmtime` crate are not affected by this issue, only users of the C API function `wasmtime_trap_code` are affected. **CVE ID : CVE-2022-39394**	t/087d9d7becf7422b3f872a3bcd5d97bb7ce7ff36	
Out-of-bounds Write	10-Nov-2022	7.4	Wasmtime is a standalone runtime for WebAssembly. Prior to version 2.0.2, there is a bug	https://github.com/bytecodealliance/wasmtime/security/advisories/	A-BYT-WASM-211122/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Wasmtime's implementation of its pooling instance allocator when the allocator is configured to give WebAssembly instances a maximum of zero pages of memory. In this configuration, the virtual memory mapping for WebAssembly memories did not meet the compiler-required configuration requirements for safely executing WebAssembly modules. Wasmtime's default settings require virtual memory page faults to indicate that wasm reads/writes are out-of-bounds, but the pooling allocator's configuration would not create an appropriate virtual memory mapping for this meaning out of bounds reads/writes can successfully read/write memory unrelated to the wasm sandbox within range of the	GHSA-44mr-8vmm-wjhg, https://github.com/bytecodealliance/wasmtime/commit/e60c3742904ccbb3e26da201c9221c38a4981d72	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			base address of the memory mapping created by the pooling allocator. This bug is not applicable with the default settings of the `wasmtime` crate. This bug can only be triggered by setting `InstanceLimits::memory_pages` to zero. This is expected to be a very rare configuration since this means that wasm modules cannot allocate any pages of linear memory. All wasm modules produced by all current toolchains are highly likely to use linear memory, so it's expected to be unlikely that this configuration is set to zero by any production embedding of Wasmtime. This bug has been patched and users should upgrade to Wasmtime 2.0.2. This bug can be worked around by increasing the `memory_pages` allotment when configuring the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pooling allocator to a value greater than zero. If an embedding wishes to still prevent memory from actually being used then the `Store::limiter` method can be used to dynamically disallow growth of memory beyond 0 bytes large. Note that the default `memory_pages` value is greater than zero. **CVE ID : CVE-2022-39392**		
Vendor: canteen_management_system_project					
Product: canteen_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	15-Nov-2022	9.8	An arbitrary file upload vulnerability in the component /pages/save_user.php of Canteen Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-43265**	N/A	A-CAN-CANT-211122/103
Improper Neutralization of Special Elements used in an	07-Nov-2022	7.2	Canteen Management System Project v1.0 was discovered to contain a SQL injection	N/A	A-CAN-CANT-211122/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			vulnerability via the component /youthappam/add-food.php. **CVE ID : CVE-2022-43049**		
Unrestricted Upload of File with Dangerous Type	09-Nov-2022	7.2	Canteen Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via ip/youthappam/php_action/editFile.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-43277**	N/A	A-CAN-CANT-211122/105
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Nov-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the categoriesId parameter at /php_action/fetchSelectedCategories.php. **CVE ID : CVE-2022-43278**	N/A	A-CAN-CANT-211122/106
Improper Neutralization of Special Elements	09-Nov-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL	N/A	A-CAN-CANT-211122/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			injection vulnerability via the id parameter at /youthappam/editcategory.php. **CVE ID : CVE-2022-43290**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Nov-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /youthappam/editclient.php. **CVE ID : CVE-2022-43291**	N/A	A-CAN-CANT-211122/108
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Nov-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /youthappam/editfood.php. **CVE ID : CVE-2022-43292**	N/A	A-CAN-CANT-211122/109
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /editorder.php.	N/A	A-CAN-CANT-211122/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43328		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /print.php. **CVE ID : CVE-2022-43329**	N/A	A-CAN-CANT-211122/111
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /editorder.php. **CVE ID : CVE-2022-43330**	N/A	A-CAN-CANT-211122/112
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.2	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php_action/printOrder.php. **CVE ID : CVE-2022-43331**	N/A	A-CAN-CANT-211122/113
Improper Neutralization of Input During Web Page	08-Nov-2022	5.4	A cross-site scripting (XSS) vulnerability in Canteen Management System v1.0 allows	N/A	A-CAN-CANT-211122/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2022-43144**		
Vendor: Centreon					
Product: centreon					
Affected Version(s): * Up to (excluding) 22.10.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Nov-2022	9.8	A vulnerability was found in centreon. It has been declared as critical. This vulnerability affects unknown code of the file formContactGroup.php of the component Contact Groups Form. The manipulation of the argument cg_id leads to sql injection. The attack can be initiated remotely. The name of the patch is 293b10628f7d9f83c6c82c78cf637cbe9b907369. It is recommended to apply a patch to fix this issue. VDB-212794 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3827**	https://github.com/centreon/centreon/pull/11869, https://github.com/centreon/centreon/commit/293b10628f7d9f83c6c82c78cf637cbe9b907369	A-CEN-CENT-211122/115
Vendor: Cisco					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: broadworks_commpilot_application					
Affected Version(s): * Up to (excluding) 23.0					
Improper Input Validation	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco BroadWorks CommPilot application could allow an unauthenticated, remote attacker to perform a server-side request forgery (SSRF) attack on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web interface. A successful exploit could allow the attacker to obtain confidential information from the BroadWorks server and other device on the network. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2022-20958**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-ssrf-BJeQfpp	A-CIS-BROA-211122/116
Product: broadworks_messaging_server					
Affected Version(s): * Up to (excluding) 23.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco BroadWorks CommPilot application could allow an authenticated, remote attacker to perform a server-side request forgery (SSRF) attack on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web interface. A successful exploit could allow the attacker to obtain confidential information from the BroadWorks server and other device on the network. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2022-20951**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-ssrf-BJeQfpp	A-CIS-BROA-211122/117
Product: email_security_appliance					
Affected Version(s): * Up to (excluding) 14.2.1-015					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	04-Nov-2022	7.5	A vulnerability in Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain TLS connections that are processed by an affected device. An attacker could exploit this vulnerability by establishing a large number of concurrent TLS connections to an affected device. A successful exploit could allow the attacker to cause the device to drop new TLS email messages that come from the associated email servers. Exploitation of this vulnerability does not cause the affected device to unexpectedly reload. The device will recover autonomously within a few hours of when the attack	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-dos-gdghHmbV	A-CIS-EMAI-211122/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is halted or mitigated. **CVE ID : CVE-2022-20960**		
Affected Version(s): From (including) 14.3.0 Up to (excluding) 14.3.0-020					
Improper Certificate Validation	04-Nov-2022	7.5	A vulnerability in Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain TLS connections that are processed by an affected device. An attacker could exploit this vulnerability by establishing a large number of concurrent TLS connections to an affected device. A successful exploit could allow the attacker to cause the device to drop new TLS email messages that come from the associated email servers. Exploitation of this vulnerability does not cause the affected device to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-dos-gdghHmbV	A-CIS-EMAI-211122/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly reload. The device will recover autonomously within a few hours of when the attack is halted or mitigated. **CVE ID : CVE-2022-20960**		
Product: identity_services_engine					
Affected Version(s): 3.0.0					
Cross-Site Request Forgery (CSRF)	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-vgNtTpAs	A-CIS-IDEN-211122/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform arbitrary actions on the affected device with the privileges of the target user. **CVE ID : CVE-2022-20961**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stor-xss-kpRBWXY	A-CIS-IDEN-211122/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid credentials to access the web-based management interface of an affected device. **CVE ID : CVE-2022-20963**		
Uncontrolled Resource Consumption	04-Nov-2022	5.3	A vulnerability in a feature that monitors RADIUS requests on Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to negatively affect the performance of an affected device. This vulnerability is due to insufficient management of system resources. An attacker could exploit this vulnerability by taking actions that cause Cisco ISE Software to receive specific RADIUS traffic. A successful and sustained exploit of this vulnerability could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-sec-atk-dos-zw5RCUYp	A-CIS-IDEN-211122/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause reduced performance of the affected device, resulting in significant delays to RADIUS authentications. There are workarounds that address this vulnerability. **CVE ID : CVE-2022-20937**		
Affected Version(s): * Up to (excluding) 2.6.0					
Cross-Site Request Forgery (CSRF)	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-vgNtTpAs	A-CIS-IDEN-211122/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the target user. **CVE ID : CVE-2022-20961**		
Affected Version(s): * Up to (excluding) 2.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stor-xss-kpRBWXY	A-CIS-IDEN-211122/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid credentials to access the web-based management interface of an affected device. **CVE ID : CVE-2022-20963**		
Uncontrolled Resource Consumption	04-Nov-2022	5.3	A vulnerability in a feature that monitors RADIUS requests on Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to negatively affect the performance of an affected device. This vulnerability is due to insufficient management of system resources. An attacker could exploit this vulnerability by taking actions that cause Cisco ISE Software to receive specific RADIUS	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-sec-atk-dos-zw5RCUYp	A-CIS-IDEN-211122/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic. A successful and sustained exploit of this vulnerability could allow the attacker to cause reduced performance of the affected device, resulting in significant delays to RADIUS authentications. There are workarounds that address this vulnerability. **CVE ID : CVE-2022-20937**		
Affected Version(s): 2.6.0					
Cross-Site Request Forgery (CSRF)	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-vgNtTpAs	A-CIS-IDEN-211122/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the target user. **CVE ID : CVE-2022-20961**		
Affected Version(s): 2.7.0					
Cross-Site Request Forgery (CSRF)	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-vgNtTpAs	A-CIS-IDEN-211122/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the target user. **CVE ID : CVE-2022-20961**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stor-xss-kpRBWXY	A-CIS-IDEN-211122/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid credentials to access the web-based management interface of an affected device. **CVE ID : CVE-2022-20963**		
Uncontrolled Resource Consumption	04-Nov-2022	5.3	A vulnerability in a feature that monitors RADIUS requests on Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to negatively affect the performance of an affected device. This vulnerability is due to insufficient management of system resources. An attacker could exploit this vulnerability by taking actions that cause Cisco ISE Software to receive specific RADIUS traffic. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-sec-atk-dos-zw5RCUYp	A-CIS-IDEN-211122/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and sustained exploit of this vulnerability could allow the attacker to cause reduced performance of the affected device, resulting in significant delays to RADIUS authentications. There are workarounds that address this vulnerability. **CVE ID : CVE-2022-20937**		
Affected Version(s): 3.1					
N/A	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to bypass authorization and access system files. This vulnerability is due to improper access control in the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx	A-CIS-IDEN-211122/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A successful exploit could allow the attacker to list, download, and delete certain files that they should not have access to. Cisco plans to release software updates that address this vulnerability. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx ["https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx"] **CVE ID : CVE-2022-20956**		
Cross-Site Request Forgery (CSRF)	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-vgNtTpAs	A-CIS-IDEN-211122/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the target user. **CVE ID : CVE-2022-20961**		
Improper Input Validation	04-Nov-2022	8.8	A vulnerability in the Localdisk Management feature of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to make unauthorized changes to the file system of an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted HTTP request with absolute path	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-path-trav-f6M7cs6r	A-CIS-IDEN-211122/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sequences. A successful exploit could allow the attacker to upload malicious files to arbitrary locations within the file system. Using this method, it is possible to access the underlying operating system and execute commands with system privileges. **CVE ID : CVE-2022-20962**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stor-xss-kpRBWXY	A-CIS-IDEN-211122/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid credentials to access the web-based management interface of an affected device. **CVE ID : CVE-2022-20963**		
Uncontrolled Resource Consumption	04-Nov-2022	5.3	A vulnerability in a feature that monitors RADIUS requests on Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to negatively affect the performance of an affected device. This vulnerability is due to insufficient management of system resources. An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-sec-atk-dos-zw5RCUYp	A-CIS-IDEN-211122/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by taking actions that cause Cisco ISE Software to receive specific RADIUS traffic. A successful and sustained exploit of this vulnerability could allow the attacker to cause reduced performance of the affected device, resulting in significant delays to RADIUS authentications. There are workarounds that address this vulnerability. **CVE ID : CVE-2022-20937**		
Affected Version(s): 3.2					
N/A	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to bypass authorization and access system files. This vulnerability is due to improper access control in the web-based management interface of an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx	A-CIS-IDEN-211122/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to list, download, and delete certain files that they should not have access to. Cisco plans to release software updates that address this vulnerability. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx ["https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx"] **CVE ID : CVE-2022-20956**		
Product: umbrella					
Affected Version(s): 003.003\\(000\\)					
Improper Neutralization of Input During Web Page Generation	04-Nov-2022	5.4	A vulnerability in multiple management dashboard pages of Cisco Umbrella could allow an authenticated, remote attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-UMBR-211122/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			conduct a cross-site scripting (XSS) attack against a user of the Cisco Umbrella dashboard. This vulnerability is due to unsanitized user input. An attacker could exploit this vulnerability by submitting custom JavaScript to the web application and persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive browser-based information. **CVE ID : CVE-2022-20969**	umbrella-xss-LfeYQV3	
Vendor: Citrix					
Product: gateway					
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-65.21					
Improper Authentication	08-Nov-2022	9.8	Unauthorized access to Gateway user capabilities **CVE ID : CVE-2022-27510**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-	A-CIT-GATE-211122/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cve20222751 3-and- cve20222751 6	
Improper Restriction of Excessive Authentica tion Attempts	08-Nov-2022	9.8	User login brute force protection functionality bypass **CVE ID : CVE-2022-27516**	https://suppo rt.citrix.com/a rticle/CTX463 706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	A-CIT-GATE-211122/138
Insufficient Verificatio n of Data Authenticit y	08-Nov-2022	9.6	Remote desktop takeover via phishing **CVE ID : CVE-2022-27513**	https://suppo rt.citrix.com/a rticle/CTX463 706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	A-CIT-GATE-211122/139
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-88.12					
Improper Authentica tion	08-Nov-2022	9.8	Unauthorized access to Gateway user capabilities **CVE ID : CVE-2022-27510**	https://suppo rt.citrix.com/a rticle/CTX463 706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-	A-CIT-GATE-211122/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cve20222751 3-and- cve20222751 6	
Improper Restriction of Excessive Authentica tion Attempts	08-Nov-2022	9.8	User login brute force protection functionality bypass **CVE ID : CVE-2022-27516**	https://suppo rt.citrix.com/a rticle/CTX463 706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	A-CIT-GATE-211122/141
Insufficient Verificatio n of Data Authenticit y	08-Nov-2022	9.6	Remote desktop takeover via phishing **CVE ID : CVE-2022-27513**	https://suppo rt.citrix.com/a rticle/CTX463 706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	A-CIT-GATE-211122/142
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-33.41					
Improper Authentica tion	08-Nov-2022	9.8	Unauthorized access to Gateway user capabilities **CVE ID : CVE-2022-27510**	https://suppo rt.citrix.com/a rticle/CTX463 706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-	A-CIT-GATE-211122/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cve20222751 3-and-cve20222751 6	
Insufficient Verification of Data Authenticity	08-Nov-2022	9.6	Remote desktop takeover via phishing **CVE ID : CVE-2022-27513**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	A-CIT-GATE-211122/144
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-33.47					
Improper Restriction of Excessive Authentication Attempts	08-Nov-2022	9.8	User login brute force protection functionality bypass **CVE ID : CVE-2022-27516**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	A-CIT-GATE-211122/145
Vendor: codeandmore					
Product: wp_page_widget					
Affected Version(s): * Up to (excluding) 4.0					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in CodeAndMore WP Page Widget plugin <= 3.9 on	https://patchstack.com/database/vulnerability/wp-page-widget/wordpress-wp-page-	A-COD-WP_P-211122/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WordPress leading to plugin settings change. **CVE ID : CVE-2022-32587**	widget-plugin-3-9-cross-site-request-forgery-csrf-vulnerability, https://wordpress.org/plugins/wp-page-widget/	
Vendor: Codection					
Product: import_and_export_users_and_customers					
Affected Version(s): * Up to (excluding) 1.20.5					
Improper Neutralization of Formula Elements in a CSV File	07-Nov-2022	8	The Import and export users and customers WordPress plugin before 1.20.5 does not properly escape data when exporting it via CSV files. **CVE ID : CVE-2022-3558**	https://plugins.trac.wordpress.org/changeset?new=2798139%40import-users-from-csv-with-meta&old=2785785%40import-users-from-csv-with-meta, https://wpscan.com/vulnerability/e3d72e04-9cdf-4b7d-953e-876e26abdfc6	A-COD-IMPO-211122/147
Vendor: coleds					
Product: simple_seo					
Affected Version(s): * Up to (including) 1.8.12					
Incorrect Authorization	03-Nov-2022	5.4	Auth. (subscriber+) Broken Access Control vulnerability in David Cole Simple SEO plugin <=	https://wordpress.org/plugins/cds-simple-seo/#developers,	A-COL-SIMP-211122/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.8.12 on WordPress allows attackers to create or delete sitemap. **CVE ID : CVE-2022-36404**	https://patchstack.com/database/vulnerability/cds-simple-seo/wordpress-simple-seo-plugin-1-8-12-authenticated-sitemap-deletion-creation-vulnerability?_s_id=cve	
Cross-Site Request Forgery (CSRF)	03-Nov-2022	5.4	Cross-Site Request Forgery (CSRF) vulnerability in David Cole Simple SEO plugin <= 1.8.12 on WordPress allows attackers to create or delete sitemaps. **CVE ID : CVE-2022-44627**	https://wordpress.org/plugins/cds-simple-seo/#developers, https://patchstack.com/database/vulnerability/cds-simple-seo/wordpress-simple-seo-plugin-1-8-12-cross-site-request-forgery-csrf-vulnerability?_s_id=cve	A-COL-SIMP-211122/149
Vendor: concretecms					
Product: concrete_cms					
Affected Version(s): * Up to (excluding) 8.5.10					
Improper Authentication	14-Nov-2022	6.3	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 did not use strict	https://github.com/concretecms/concretecms/releases/8.5.10, https://docu	A-CON-CONC-211122/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			comparison for the legacy_salt so that limited authentication bypass could occur if using this functionality. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+. **CVE ID : CVE-2022-43690**	mentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	6.1	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Reflected XSS - user can cause an administrator to trigger reflected XSS with a url if the targeted administrator is using an old browser that lacks XSS protection. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+. **CVE ID : CVE-2022-43692**	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	A-CON-CONC-211122/151
Improper Neutralization of Input During Web Page	14-Nov-2022	6.1	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to	https://github.com/concretecms/concretecms/releases/8.5.10, https://docu	A-CON-CONC-211122/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Reflected XSS in the image manipulation library due to un-sanitized output. **CVE ID : CVE-2022-43694**	mentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	
Improper Restriction of XML External Entity Reference	14-Nov-2022	5.3	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to XXE based DNS requests leading to IP disclosure. **CVE ID : CVE-2022-43689**	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	A-CON-CONC-211122/153
Improper Neutralization of Input During Web Page Generation	14-Nov-2022	4.8	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Stored Cross-Site	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.con	A-CON-CONC-211122/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting (XSS) in icons since the Microsoft application tile color is not sanitized. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+. **CVE ID : CVE-2022-43688**	cretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Nov-2022	4.8	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Stored Cross-Site Scripting (XSS) in dashboard/system/express/entities/associations because Concrete CMS allows association with an entity name that doesn't exist or, if it does exist, contains XSS since it was not properly sanitized. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+. **CVE ID : CVE-2022-43695**	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	A-CON-CONC-211122/155
Affected Version(s): From (including) 9.0.0 Up to (including) 9.1.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	14-Nov-2022	6.3	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 did not use strict comparison for the legacy_salt so that limited authentication bypass could occur if using this functionality. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+. **CVE ID : CVE-2022-43690**	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	A-CON-CONC-211122/156
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	6.1	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Reflected XSS - user can cause an administrator to trigger reflected XSS with a url if the targeted administrator is using an old browser that lacks XSS protection. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+. **CVE ID : CVE-2022-43692**	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	A-CON-CONC-211122/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	6.1	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Reflected XSS in the image manipulation library due to un-sanitized output. **CVE ID : CVE-2022-43694**	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	A-CON-CONC-211122/158
Improper Restriction of XML External Entity Reference	14-Nov-2022	5.3	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to XXE based DNS requests leading to IP disclosure. **CVE ID : CVE-2022-43689**	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	A-CON-CONC-211122/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	4.8	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Stored Cross-Site Scripting (XSS) in icons since the Microsoft application tile color is not sanitized. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+. **CVE ID : CVE-2022-43688**	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	A-CON-CONC-211122/160
Improper Neutralization of Special Elements used in a Command ('Command Injection')	14-Nov-2022	4.8	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Stored Cross-Site Scripting (XSS) in dashboard/system/express/entities/associations because Concrete CMS allows association with an entity name that doesn't exist or, if it does exist, contains XSS since it was not properly sanitized. Remediate by updating to	https://github.com/concretecms/concretecms/releases/8.5.10, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes	A-CON-CONC-211122/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Concrete CMS 9.1.3+ or 8.5.10+. **CVE ID : CVE-2022-43695**		
Vendor: crm42_project					
Product: crm42					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Nov-2022	9.8	A vulnerability was found in tholum crm42. It has been rated as critical. This issue affects some unknown processing of the file crm42\class\class.user.php of the component Login. The manipulation of the argument user_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213461 was assigned to this vulnerability. **CVE ID : CVE-2022-3955**	N/A	A-CRM-CRM4-211122/162
Vendor: Csphere					
Product: clansphere					
Affected Version(s): 2011.4					
Improper Neutralization of Input	09-Nov-2022	6.1	A cross-site scripting (XSS) vulnerability in Clansphere CMS	N/A	A-CSP-CLAN-211122/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			v2011.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Username parameter. **CVE ID : CVE-2022-43119**		
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): 6.1.9					
Cross-Site Request Forgery (CSRF)	09-Nov-2022	8.8	DedeCMS v6.1.9 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily add Administrator accounts and modify Admin passwords. **CVE ID : CVE-2022-43031**	N/A	A-DED-DEDE-211122/164
Vendor: deep-object-diff_project					
Product: deep-object-diff					
Affected Version(s): 1.1.0					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	03-Nov-2022	5.3	deep-object-diff version 1.1.0 allows an external attacker to edit or add new properties to an object. This is possible because the application does not properly validate incoming JSON keys, thus allowing the	N/A	A-DEE-DEEP-211122/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'__proto__' property to be edited. **CVE ID : CVE-2022-41713**		
Vendor: deep-parse-json_project					
Product: deep-parse-json					
Affected Version(s): 1.0.2					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	03-Nov-2022	5.3	deep-parse-json version 1.0.2 allows an external attacker to edit or add new properties to an object. This is possible because the application does not correctly validate the incoming JSON keys, thus allowing the '__proto__' property to be edited. **CVE ID : CVE-2022-42743**	N/A	A-DEE-DEEP-211122/166
Vendor: democritus					
Product: d8s-dates					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	9.8	The d8s-dates for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-timezones package. The affected	N/A	A-DEM-D8S--211122/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-44052**		
Product: d8s-networking					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	9.8	The d8s-networking for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-json package. The affected version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-44050**	N/A	A-DEM-D8S--211122/168
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	9.8	The d8s-networking for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-user-agents package. The affected version of d8s-htm is 0.1.0.	N/A	A-DEM-D8S--211122/169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44053		
Product: d8s-python					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	9.8	The d8s-python for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-algorithms package. The affected version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-43305**	N/A	A-DEM-D8S--211122/170
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	9.8	The d8s-python for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-grammars package. The affected version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-44049**	N/A	A-DEM-D8S--211122/171
Product: d8s-stats					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	9.8	The d8s-stats for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-math package. The affected version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-44051**	N/A	A-DEM-D8S--211122/172
Product: d8s-strings					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	9.8	The d8s-strings for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-uuids package. The affected version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-43303**	N/A	A-DEM-D8S--211122/173
Product: d8s-timer					
Affected Version(s): 0.1.0					
Unrestricted Upload of	07-Nov-2022	9.8	The d8s-timer for python, as	N/A	A-DEM-D8S--211122/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-uuids package. The affected version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-43304**		
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	8.8	The d8s-timer for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-dates package. The affected version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-43306**	N/A	A-DEM-D8S--211122/175
Product: d8s-urls					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	9.8	The d8s-urls for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code	N/A	A-DEM-D8S--211122/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution backdoor inserted by third parties is the democritus-domains package. The affected version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-44048**		
Product: d8s-xml					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	9.8	The d8s-xml for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-utility package. The affected version of d8s-htm is 0.1.0. **CVE ID : CVE-2022-44054**	https://pypi.org/project/democritus-utility/, https://pypi.org/project/d8s-xml/	A-DEM-D8S--211122/177
Vendor: devolutions					
Product: devolutions_server					
Affected Version(s): * Up to (excluding) 2022.3.2					
Missing Encryption of Sensitive Data	01-Nov-2022	6.5	Dashlane password and Keepass Server password in My Account Settings are not encrypted in the database in Devolutions Remote Desktop Manager 2022.2.26	https://devolutions.net/security/advisories/DEVO-2022-0009	A-DEV-DEVO-211122/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior versions and Devolutions Server 2022.3.1 and prior versions which allows database users to read the data. This issue affects : Remote Desktop Manager 2022.2.26 and prior versions. Devolutions Server 2022.3.1 and prior versions. **CVE ID : CVE-2022-3781**		
Product: remote_desktop_manager					
Affected Version(s): * Up to (excluding) 2022.2.27					
Missing Encryption of Sensitive Data	01-Nov-2022	6.5	Dashlane password and Keepass Server password in My Account Settings are not encrypted in the database in Devolutions Remote Desktop Manager 2022.2.26 and prior versions and Devolutions Server 2022.3.1 and prior versions which allows database users to read the data. This issue affects : Remote Desktop Manager 2022.2.26 and prior versions. Devolutions Server 2022.3.1 and prior versions.	https://devolutions.net/security/advisories/DEVO-2022-0009	A-DEV-REMO-211122/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3781		
Affected Version(s): * Up to (excluding) 2022.3.8					
Incorrect Authorization	01-Nov-2022	7.5	Database connections on deleted users could stay active on MySQL data sources in Remote Desktop Manager 2022.3.7 and below which allow deleted users to access unauthorized data. This issue affects : Remote Desktop Manager 2022.3.7 and prior versions. **CVE ID : CVE-2022-3780**	https://devolutions.net/security/advisories/DEVO-2022-0008	A-DEV-REMO-211122/180
Vendor: diagrams					
Product: drawio					
Affected Version(s): * Up to (excluding) 20.5.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Nov-2022	6.1	Cross-site Scripting (XSS) - DOM in GitHub repository jgraph/drawio prior to 20.5.2. **CVE ID : CVE-2022-3873**	https://huntr.dev/bounties/52a4085e-b687-489b-9ed6-f0987583ed77, https://github.com/jgraph/drawio/commit/d37894baf125430e85840c2635563b10d1a6523d	A-DIA-DRAW-211122/181
Vendor: digitialpixies					
Product: oauth_client					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.1.0					
Cross-Site Request Forgery (CSRF)	14-Nov-2022	6.5	The OAuth Client by DigitialPixies WordPress plugin through 1.1.0 does not have CSRF checks in some places, which could allow attackers to make logged-in users perform unwanted actions. **CVE ID : CVE-2022-3632**	https://wpscan.com/vulnerability/4c1b0e5e-245a-4d1f-a561-e91af906e62d	A-DIG-OAUT-211122/182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	4.8	The OAuth Client by DigitialPixies WordPress plugin through 1.1.0 does not sanitize and escapes 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-2022-3631**	https://wpscan.com/vulnerability/13966b61-7e65-4493-8bd8-828d6d4441d5	A-DIG-OAUT-211122/183
Vendor: discourse					
Product: discourse					
Affected Version(s): * Up to (excluding) 2.8.10					
Incorrect Authorization	02-Nov-2022	8.8	Discourse is a platform for community discussion. Users	https://github.com/discourse/discourse/security/advis	A-DIS-DISC-211122/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			who receive an invitation link that is not scoped to a single email address can enter any non-admin user's email and gain access to their account when accepting the invitation. All users should upgrade to the latest version. A workaround is temporarily disabling invitations with `SiteSetting.max_invites_per_day = 0` or scope them to individual email addresses. **CVE ID : CVE-2022-39356**	ories/GHSA-x8w7-rwmr-w278, https://github.com/discourse/discourse/pull/18817	
Server-Side Request Forgery (SSRF)	02-Nov-2022	4.9	Discourse is a platform for community discussion. A malicious admin could use this vulnerability to perform port enumeration on the local host or other hosts on the internal network, as well as against hosts on the Internet. Latest `stable`, `beta`, and `test-passed` versions are now patched. As a	https://github.com/discourse/discourse/security/advisories/GHSA-rcc5-28r3-23rr	A-DIS-DISC-211122/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workaround, self-hosters can use `DISCOURSE_BLOCKED_IP_BLOCKS` env var (which overrides `blocked_ip_blocks` setting) to stop webhooks from accessing private IPs. **CVE ID : CVE-2022-39241**		
Affected Version(s): * Up to (excluding) 2.8.9					
N/A	02-Nov-2022	5.3	Discourse is a platform for community discussion. Under certain conditions, a user badge may have been awarded based on a user's activity in a topic with restricted access. Before this vulnerability was disclosed, the topic title of the topic associated with the user badge may be viewed by any user. If there are sensitive information in the topic title, it will therefore have been exposed. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. There are currently no	https://github.com/discourse/discourse/security/advisories/GHSA-2gvq-27h6-4h5f	A-DIS-DISC-211122/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds available. **CVE ID : CVE-2022-39378**		
Affected Version(s): 2.9.0					
Incorrect Authorization	02-Nov-2022	8.8	Discourse is a platform for community discussion. Users who receive an invitation link that is not scoped to a single email address can enter any non-admin user's email and gain access to their account when accepting the invitation. All users should upgrade to the latest version. A workaround is temporarily disabling invitations with `SiteSetting.max_invites_per_day = 0` or scope them to individual email addresses. **CVE ID : CVE-2022-39356**	https://github.com/discourse/discourse/security/advisories/GHSA-x8w7-rwmr-w278, https://github.com/discourse/discourse/pull/18817	A-DIS-DISC-211122/187
N/A	02-Nov-2022	5.3	Discourse is a platform for community discussion. Under certain conditions, a user badge may have been awarded based on a user's	https://github.com/discourse/discourse/security/advisories/GHSA-2gvq-27h6-4h5f	A-DIS-DISC-211122/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			activity in a topic with restricted access. Before this vulnerability was disclosed, the topic title of the topic associated with the user badge may be viewed by any user. If there are sensitive information in the topic title, it will therefore have been exposed. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. There are currently no known workarounds available. **CVE ID : CVE-2022-39378**		
Server-Side Request Forgery (SSRF)	02-Nov-2022	4.9	Discourse is a platform for community discussion. A malicious admin could use this vulnerability to perform port enumeration on the local host or other hosts on the internal network, as well as against hosts on the Internet. Latest `stable`, `beta`, and `test-passed`	https://github.com/discourse/discourse/security/advisories/GHSA-rcc5-28r3-23rr	A-DIS-DISC-211122/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions are now patched. As a workaround, self-hosters can use `DISCOURSE_BLOCKED_IP_BLOCKS` env var (which overrides `blocked_ip_blocks` setting) to stop webhooks from accessing private IPs. **CVE ID : CVE-2022-39241**		
Vendor: Dotcms					
Product: dotcms					
Affected Version(s): From (including) 21.06 Up to (excluding) 21.06.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	6.1	dotCMS before 22.06 allows remote attackers to bypass intended access control and obtain sensitive information by using a semicolon in a URL to introduce a matrix parameter. (This is also fixed in 5.3.8.12, 21.06.9, and 22.03.2 for LTS users.) Some Java application frameworks, including those used by Spring or Tomcat, allow the use of matrix parameters: these are URI parameters separated by	https://www.dotcms.com/security/SI-63	A-DOT-DOTC-211122/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			semicolons. Through precise semicolon placement in a URI, it is possible to exploit this feature to avoid dotCMS's path-based XSS prevention (such as "require login" filters), and consequently access restricted resources. For example, an attacker could place a semicolon immediately before a / character that separates elements of a filesystem path. This could reveal file content that is ordinarily only visible to signed-in users. This issue can be chained with other exploit code to achieve XSS attacks against dotCMS. **CVE ID : CVE-2022-35740**		
Affected Version(s): From (including) 22.01 Up to (excluding) 22.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	6.1	dotCMS before 22.06 allows remote attackers to bypass intended access control and obtain sensitive information by using a semicolon in a URL to	https://www.dotcms.com/security/SI-63	A-DOT-DOTC-211122/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			introduce a matrix parameter. (This is also fixed in 5.3.8.12, 21.06.9, and 22.03.2 for LTS users.) Some Java application frameworks, including those used by Spring or Tomcat, allow the use of matrix parameters: these are URI parameters separated by semicolons. Through precise semicolon placement in a URI, it is possible to exploit this feature to avoid dotCMS's path-based XSS prevention (such as "require login" filters), and consequently access restricted resources. For example, an attacker could place a semicolon immediately before a / character that separates elements of a filesystem path. This could reveal file content that is ordinarily only visible to signed-in users. This issue can be chained with other exploit code to achieve XSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against dotCMS. **CVE ID : CVE-2022-35740**		
Affected Version(s): From (including) 22.03 Up to (excluding) 22.03.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	6.1	dotCMS before 22.06 allows remote attackers to bypass intended access control and obtain sensitive information by using a semicolon in a URL to introduce a matrix parameter. (This is also fixed in 5.3.8.12, 21.06.9, and 22.03.2 for LTS users.) Some Java application frameworks, including those used by Spring or Tomcat, allow the use of matrix parameters: these are URI parameters separated by semicolons. Through precise semicolon placement in a URI, it is possible to exploit this feature to avoid dotCMS's path-based XSS prevention (such as "require login" filters), and consequently access restricted resources. For	https://www.dotcms.com/security/SI-63	A-DOT-DOTC-211122/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example, an attacker could place a semicolon immediately before a / character that separates elements of a filesystem path. This could reveal file content that is ordinarily only visible to signed-in users. This issue can be chained with other exploit code to achieve XSS attacks against dotCMS. **CVE ID : CVE-2022-35740**		
Affected Version(s): From (including) 5.3.8 Up to (excluding) 5.3.8.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	6.1	dotCMS before 22.06 allows remote attackers to bypass intended access control and obtain sensitive information by using a semicolon in a URL to introduce a matrix parameter. (This is also fixed in 5.3.8.12, 21.06.9, and 22.03.2 for LTS users.) Some Java application frameworks, including those used by Spring or Tomcat, allow the use of matrix parameters: these are URI parameters	https://www.dotcms.com/security/SI-63	A-DOT-DOTC-211122/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			separated by semicolons. Through precise semicolon placement in a URI, it is possible to exploit this feature to avoid dotCMS's path-based XSS prevention (such as "require login" filters), and consequently access restricted resources. For example, an attacker could place a semicolon immediately before a / character that separates elements of a filesystem path. This could reveal file content that is ordinarily only visible to signed-in users. This issue can be chained with other exploit code to achieve XSS attacks against dotCMS. **CVE ID : CVE-2022-35740**		
Vendor: drogon					
Product: drogon					
Affected Version(s): * Up to (excluding) 1.8.2					
Use of Insufficiently Random Values	11-Nov-2022	5.3	A vulnerability, which was classified as problematic, has been found in	https://github.com/drogonframework/drogon/commit/c0d48da99f6	A-DRO-DROG-211122/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drogon up to 1.8.1. Affected by this issue is some unknown functionality of the component Session Hash Handler. The manipulation leads to small space of random values. The attack may be launched remotely. Upgrading to version 1.8.2 is able to address this issue. The name of the patch is c0d48da99f66aaada17bcd28b07741cac8697647. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-213464. **CVE ID : CVE-2022-3959**	6aaada17bcd28b07741cac8697647, https://github.com/drogonframework/drogon/pull/1433	
Vendor: ecisp					
Product: espcms					
Affected Version(s): p8.21120101					
N/A	10-Nov-2022	9.8	ESPCMS P8.21120101 was discovered to contain a remote code execution (RCE) vulnerability in the component UPFILE_PIC_ZOOM_HIGHT.	N/A	A-ECI-ESPC-211122/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44087		
N/A	10-Nov-2022	9.8	ESPCMS P8.21120101 was discovered to contain a remote code execution (RCE) vulnerability in the component INPUT_ISDESCRIPTION. **CVE ID : CVE-2022-44088**	N/A	A-ECI-ESPC-211122/196
N/A	10-Nov-2022	9.8	ESPCMS P8.21120101 was discovered to contain a remote code execution (RCE) vulnerability in the component IS_GETCACHE. **CVE ID : CVE-2022-44089**	N/A	A-ECI-ESPC-211122/197
Vendor: Eclipse					
Product: deeplearning4j					
Affected Version(s): * Up to (excluding) 1.0.0					
Use of Insufficiently Random Values	10-Nov-2022	5.3	Deeplearning4J is a suite of tools for deploying and training deep learning models using the JVM. Packages org.deeplearning4j:dl4j-examples and org.deeplearning4j:platform-tests through version 1.0.0-M2.1 may use some unclaimed S3 buckets in tests in	https://github.com/eclipse/deeplearning4j/security/advisories/GHSA-rc39-g977-687w	A-ECL-DEEP-211122/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			examples. This is likely affect people who use some older NLP examples that reference an old S3 bucket. The problem has been patched. Users should upgrade to snapshots as Deeplearning4J plan to publish a release with the fix at a later date. As a workaround, download a word2vec google news vector from a new source using git lfs from here. **CVE ID : CVE-2022-36022**		
Affected Version(s): 1.0.0					
Use of Insufficiently Random Values	10-Nov-2022	5.3	Deeplearning4J is a suite of tools for deploying and training deep learning models using the JVM. Packages org.deeplearning4j:dl4j-examples and org.deeplearning4j:platform-tests through version 1.0.0-M2.1 may use some unclaimed S3 buckets in tests in examples. This is likely affect people who use some older NLP examples that reference an old S3	https://github.com/eclipse/deeplearning4j/security/advisories/GHSA-rc39-g977-687w	A-ECL-DEEP-211122/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bucket. The problem has been patched. Users should upgrade to snapshots as Deeplearning4J plan to publish a release with the fix at a later date. As a workaround, download a word2vec google news vector from a new source using git lfs from here. **CVE ID : CVE-2022-36022**		
Vendor: electronjs					
Product: electron					
Affected Version(s): * Up to (excluding) 18.3.7					
Insufficiently Protected Credentials	08-Nov-2022	6.1	The Electron framework enables writing cross-platform desktop applications using JavaScript, HTML and CSS. In versions prior to 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7, Electron is vulnerable to Exposure of Sensitive Information. When following a redirect, Electron delays a check for redirecting to file:// URLs from other schemes. The contents of the file	https://github.com/electron/electron/security/advisories/GHSA-p2jh-44qj-pf2v	A-ELE-ELEC-211122/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is not available to the renderer following the redirect, but if the redirect target is a SMB URL such as `file://some.website.com/`, then in some cases, Windows will connect to that server and attempt NTLM authentication, which can include sending hashed credentials.This issue has been patched in versions: 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7. Users are recommended to upgrade to the latest stable version of Electron. If upgrading isn't possible, this issue can be addressed without upgrading by preventing redirects to file:// URLs in the `WebContents.on('will-redirect')` event, for all WebContents as a workaround. **CVE ID : CVE-2022-36077**		
Affected Version(s): 21.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	08-Nov-2022	6.1	The Electron framework enables writing cross-platform desktop applications using JavaScript, HTML and CSS. In versions prior to 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7, Electron is vulnerable to Exposure of Sensitive Information. When following a redirect, Electron delays a check for redirecting to file:// URLs from other schemes. The contents of the file is not available to the renderer following the redirect, but if the redirect target is a SMB URL such as `file://some.website.com/`, then in some cases, Windows will connect to that server and attempt NTLM authentication, which can include sending hashed credentials.This issue has been patched in versions: 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7.	https://github.com/electron/electron/security/advisories/GHSA-p2jh-44qj-pf2v	A-ELE-ELEC-211122/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Users are recommended to upgrade to the latest stable version of Electron. If upgrading isn't possible, this issue can be addressed without upgrading by preventing redirects to file:// URLs in the `WebContents.on('will-redirect')` event, for all WebContents as a workaround. **CVE ID : CVE-2022-36077**		
Affected Version(s): From (including) 19.0.0 Up to (excluding) 19.0.11					
Insufficiently Protected Credentials	08-Nov-2022	6.1	The Electron framework enables writing cross-platform desktop applications using JavaScript, HTML and CSS. In versions prior to 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7, Electron is vulnerable to Exposure of Sensitive Information. When following a redirect, Electron delays a check for redirecting to file:// URLs from other schemes. The contents of the file is not available to	https://github.com/electron/electron/security/advisories/GHSA-p2jh-44qj-pf2v	A-ELE-ELEC-211122/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the renderer following the redirect, but if the redirect target is a SMB URL such as `file://some.website.com/`, then in some cases, Windows will connect to that server and attempt NTLM authentication, which can include sending hashed credentials.This issue has been patched in versions: 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7. Users are recommended to upgrade to the latest stable version of Electron. If upgrading isn't possible, this issue can be addressed without upgrading by preventing redirects to file:// URLs in the `WebContents.on('will-redirect')` event, for all WebContents as a workaround. **CVE ID : CVE-2022-36077**		
Affected Version(s): From (including) 20.0.0 Up to (excluding) 20.0.1					
Insufficiently	08-Nov-2022	6.1	The Electron framework enables	https://github.com/electron	A-ELE-ELEC-211122/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			writing cross-platform desktop applications using JavaScript, HTML and CSS. In versions prior to 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7, Electron is vulnerable to Exposure of Sensitive Information. When following a redirect, Electron delays a check for redirecting to file:// URLs from other schemes. The contents of the file is not available to the renderer following the redirect, but if the redirect target is a SMB URL such as `file://some.website.com/`, then in some cases, Windows will connect to that server and attempt NTLM authentication, which can include sending hashed credentials.This issue has been patched in versions: 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7. Users are recommended to	/electron/security/advisories/GHSA-p2jh-44qj-pf2v	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to the latest stable version of Electron. If upgrading isn't possible, this issue can be addressed without upgrading by preventing redirects to file:// URLs in the `WebContents.on('will-redirect')` event, for all WebContents as a workaround. **CVE ID : CVE-2022-36077**		
Vendor: element					
Product: element					
Affected Version(s): * Up to (excluding) 1.9.7					
N/A	11-Nov-2022	6.5	Element iOS is an iOS Matrix client provided by Element. It is based on MatrixSDK. Prior to version 1.9.7, events encrypted using Megolm for which trust could not be established did not get decorated accordingly (with warning shields). Therefore a malicious homeserver could inject messages into the room without the user being alerted that the messages were	https://github.com/vector-im/element-ios/security/advisories/GHSA-fm8m-99j7-323g	A-ELE-ELEM-211122/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not sent by a verified group member, even if the user has previously verified all group members. This issue has been patched in Element iOS 1.9.7. There are currently no known workarounds. **CVE ID : CVE-2022-41904**		
Vendor: emlog					
Product: emlog					
Affected Version(s): 1.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	4.8	Emlog Pro v1.7.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability at /admin/store.php. **CVE ID : CVE-2022-43372**	N/A	A-EML-EMLO-211122/205
Vendor: eolink					
Product: apinto-dashboard					
Affected Version(s): -					
URL Redirection to Untrusted Site ('Open Redirect')	01-Nov-2022	6.1	A vulnerability was found in eolinker apinto-dashboard. It has been rated as problematic. This issue affects some unknown processing of the file /login. The manipulation of the argument callback leads to open redirect. The attack	N/A	A-EOL-APIN-211122/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212633 was assigned to this vulnerability. **CVE ID : CVE-2022-3797**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-2022	6.1	A vulnerability was found in eolinker apinto-dashboard and classified as problematic. This issue affects some unknown processing of the file /api/discoveries/. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212639. **CVE ID : CVE-2022-3803**	N/A	A-EOL-APIN-211122/207
Improper Neutralization of Input During Web Page Generation	01-Nov-2022	6.1	A vulnerability was found in eolinker apinto-dashboard. It has been classified as problematic. Affected is an	N/A	A-EOL-APIN-211122/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			unknown function of the file /login. The manipulation of the argument callback leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212640. **CVE ID : CVE-2022-3804**		
Product: goku_lite					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Nov-2022	9.8	A vulnerability classified as critical has been found in eolinker goku_lite. This affects an unknown part of the file /balance/service/list. The manipulation of the argument route/keyword 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-213453 was	N/A	A-EOL-GOKU-211122/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2022-3947**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Nov-2022	9.8	A vulnerability classified as critical was found in eolinker goku_lite. This vulnerability affects unknown code of the file /plugin/getList. The manipulation of the argument route/keyword leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-213454 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3948**	N/A	A-EOL-GOKU-211122/210
Vendor: eramba					
Product: eramba					
Affected Version(s): c2.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	5.4	A stored cross-site scripting (XSS) vulnerability in the Add function of Eramba GRC Software c2.8.1 allows attackers to execute arbitrary web scripts or HTML via a crafted	https://discussions.eramba.org/t/question-stored-xss-vulnerability/2326, https://www.eramba.org/	A-ERA-ERAM-211122/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload injected into the KPI Title text field. **CVE ID : CVE-2022-43342**		
Vendor: erp_project					
Product: erp					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	11-Nov-2022	8.8	A vulnerability was found in jerryhanjj ERP. It has been declared as critical. Affected by this vulnerability is the function uploadImages of the file application/controllers/basedata/inventory.php of the component Commodity Management. The manipulation leads to unrestricted upload. 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-213451. **CVE ID : CVE-2022-3944**	N/A	A-ERP-ERP-211122/212
Vendor: etictelecom					
Product: remote_access_server					
Affected Version(s): * Up to (including) 4.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Nov-2022	7.5	All versions of ETIC Telecom Remote Access Server (RAS) 4.5.0 and prior's application programmable interface (API) is vulnerable to directory traversal through several different methods. This could allow an attacker to read sensitive files from the server, including SSH private keys, passwords, scripts, python objects, database files, and more. **CVE ID : CVE-2022-41607**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-307-01	A-ETI-REMO-211122/213
Insufficient Verification of Data Authenticity	10-Nov-2022	10	All versions of ETIC Telecom Remote Access Server (RAS) 4.5.0 and prior's web portal is vulnerable to accepting malicious firmware packages that could provide a backdoor to an attacker and provide privilege escalation to the device. **CVE ID : CVE-2022-3703**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-307-01	A-ETI-REMO-211122/214
Unrestricted Upload of File with	10-Nov-2022	10	All versions of ETIC Telecom Remote Access Server (RAS) 4.5.0 and	https://www.cisa.gov/uscert/ics/advisori	A-ETI-REMO-211122/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			prior is vulnerable to malicious file upload. An attacker could take advantage of this to store malicious files on the server, which could override sensitive and useful existing files on the filesystem, fill the hard disk to full capacity, or compromise the affected device or computers with administrator level privileges connected to the affected device. **CVE ID : CVE-2022-40981**	es/icsa-22-307-01	
Vendor: Exiv2					
Product: exiv2					
Affected Version(s): * Up to (excluding) 2022-10-27					
Improper Resource Shutdown or Release	11-Nov-2022	6.5	A vulnerability was found in Exiv2. It has been classified as problematic. This affects the function QuickTimeVideo::multipleEntriesDecoder of the file quicktimevideo.cpp of the component QuickTime Video Handler. The manipulation leads to infinite loop. It is possible to initiate	https://github.com/Exiv2/exiv2/pull/2394, https://github.com/Exiv2/exiv2/commit/771ead87321ae6e39e5c9f6f0855c58cde6648f1	A-EXI-EXIV-211122/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attack remotely. The name of the patch is 771ead87321ae6e39e5c9f6f0855c58cde6648f1. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-213459. **CVE ID : CVE-2022-3953**		
Vendor: Eyesofnetwork					
Product: web_interface					
Affected Version(s): 5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	EyesOfNetwork Web Interface v5.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /lilac/main.php. **CVE ID : CVE-2022-41434**	N/A	A-EYE-WEB_-211122/217
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	4.8	EyesOfNetwork Web Interface v5.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /module/report_event/index.php. **CVE ID : CVE-2022-41432**	N/A	A-EYE-WEB_-211122/218
Improper Neutralizat	08-Nov-2022	4.8	EyesOfNetwork Web Interface v5.3	N/A	A-EYE-WEB_-211122/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /module/admin_bp/add_application.php. **CVE ID : CVE-2022-41433**		
Vendor: eyoucms					
Product: eyoucms					
Affected Version(s): 1.5.9					
Cross-Site Request Forgery (CSRF)	14-Nov-2022	8.8	EyouCMS V1.5.9-UTF8-SP1 was discovered to contain a Cross-Site Request Forgery (CSRF) via the Top Up Balance component under the Edit Member module. **CVE ID : CVE-2022-43323**	N/A	A-EYO-EYOU-211122/220
Cross-Site Request Forgery (CSRF)	14-Nov-2022	8.8	EyouCMS V1.5.9-UTF8-SP1 was discovered to contain a Cross-Site Request Forgery (CSRF) via the Basic Information component under the Edit Member module. **CVE ID : CVE-2022-44387**	N/A	A-EYO-EYOU-211122/221
Cross-Site Request Forgery (CSRF)	14-Nov-2022	6.5	EyouCMS V1.5.9-UTF8-SP1 was discovered to contain a Cross-Site	N/A	A-EYO-EYOU-211122/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Forgery (CSRF) via the Edit Admin Profile module. This vulnerability allows attackers to arbitrarily change Administrator account information. **CVE ID : CVE-2022-44389**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	5.4	A cross-site scripting (XSS) vulnerability in EyouCMS V1.5.9-UTF8-SP1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Public Security Record Number text field. **CVE ID : CVE-2022-44390**	N/A	A-EYO-EYOU-211122/223
Vendor: F-secure					
Product: safe					
Affected Version(s): * Up to (including) 19.0					
N/A	07-Nov-2022	6.5	WithSecure through 2022-08-10 allows attackers to cause a denial of service (issue 3 of 5). **CVE ID : CVE-2022-38164**	https://www.f-secure.com/en/home/support/security-advisories	A-F-S-SAFE-211122/224
N/A	07-Nov-2022	3.5	A Drag and Drop spoof vulnerability was discovered in	https://www.f-secure.com/e	A-F-S-SAFE-211122/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F-Secure SAFE Browser for Android and iOS version 19.0 and below. Drag and drop operation by user on address bar could lead to a spoofing of the address bar. **CVE ID : CVE-2022-38163**	n/home/support/security-advisories, https://withsecure.com, https://www.f-secure.com/en/home/support/security-advisories/cve-2022-38163	
Vendor: Facebook					
Product: redex					
Affected Version(s): * Up to (excluding) 2022-11-04					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Nov-2022	9.8	DexLoader function get_stringidx_fromdex() in Redex prior to commit 3b44c64 can load an out of bound address when loading the string index table, potentially allowing remote code execution during processing of a 3rd party Android APK file. **CVE ID : CVE-2022-36938**	https://github.com/facebook/redex/commit/3b44c640346b77bfb7ef36e2413688dd460288d2	A-FAC-REDE-211122/226
Vendor: fastest-json-copy_project					
Product: fastest-json-copy					
Affected Version(s): 1.0.1					
Improperly Controlled Modification of Object Prototype Attributes	03-Nov-2022	5.3	fastest-json-copy version 1.0.1 allows an external attacker to edit or add new properties to an object. This is possible because	N/A	A-FAS-FAST-211122/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Prototype Pollution')			the application does not correctly validate the incoming JSON keys, thus allowing the '__proto__' property to be edited. **CVE ID : CVE-2022-41714**		
Vendor: fastify					
Product: websocket					
Affected Version(s): 5.0.0					
N/A	08-Nov-2022	7.5	@fastify/websocket provides WebSocket support for Fastify. Any application using @fastify/websocket could crash if a specific, malformed packet is sent. All versions of fastify-websocket are also impacted. That module is deprecated, so it will not be patched. This has been patched in version 7.1.1 (fastify v4) and version 5.0.1 (fastify v3). There are currently no known workarounds. However, it should be possible to attach the error handler manually. The recommended path is upgrading	https://github.com/fastify/fastify-websocket/security/advisories/GHSA-4pcg-wr6c-h9cq	A-FAS-WEBS-211122/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the patched versions. **CVE ID : CVE-2022-39386**		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 7.1.1					
N/A	08-Nov-2022	7.5	@fastify/websocket provides WebSocket support for Fastify. Any application using @fastify/websocket could crash if a specific, malformed packet is sent. All versions of fastify-websocket are also impacted. That module is deprecated, so it will not be patched. This has been patched in version 7.1.1 (fastify v4) and version 5.0.1 (fastify v3). There are currently no known workarounds. However, it should be possible to attach the error handler manually. The recommended path is upgrading to the patched versions. **CVE ID : CVE-2022-39386**	https://github.com/fastify/fastify-websocket/security/advisories/GHSA-4pcg-wr6c-h9cq	A-FAS-WEBS-211122/229
Vendor: fast_food_ordering_system_project					
Product: fast_food_ordering_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.5	Fast Food Ordering System v1.0 was discovered to contain a SQL injection vulnerability via the component /fastfood/purchase.php. **CVE ID : CVE-2022-43081**	N/A	A-FAS-FAST-211122/230
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-2022	6.1	A cross-site scripting (XSS) vulnerability in /fastfood/purchase.php of Fast Food Ordering System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the customer parameter. **CVE ID : CVE-2022-43082**	N/A	A-FAS-FAST-211122/231
Vendor: fatcatapps					
Product: analytics_cat					
Affected Version(s): * Up to (excluding) 1.1.0					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Fatcat Apps Analytics Cat plugin <= 1.0.9 on WordPress allows Plugin Settings Change. **CVE ID : CVE-2022-27855**	https://wordpress.org/plugins/analytics-cat/#developers, https://patchstack.com/database/vulnerability/analytics-cat/wordpres	A-FAT-ANAL-211122/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				s-analytics-cat-plugin-1-0-9-plugin-settings-change-via-cross-site-request-forgery-csrf-vulnerability?_s_id=cve	
Vendor: feehi					
Product: feehicms					
Affected Version(s): 2.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-2022	6.1	FeehiCMS v2.1.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the id parameter at /web/admin/index.php?r=log%2Fview-layer. **CVE ID : CVE-2022-43320**	N/A	A-FEE-FEEH-211122/233
Vendor: ferry_project					
Product: ferry					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Nov-2022	9.8	A vulnerability, which was classified as critical, has been found in lanyulei ferry. Affected by this issue is some unknown functionality of the file apis/public/file.go of the component API. The	N/A	A-FER-FERR-211122/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument file leads to path traversal. The attack may be launched remotely. VDB-213446 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3939**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Nov-2022	9.8	A vulnerability, which was classified as problematic, was found in lanyulei ferry. This affects an unknown part of the file apis/process/task.go. The manipulation of the argument file_name leads to path traversal. The associated identifier of this vulnerability is VDB-213447. **CVE ID : CVE-2022-3940**	N/A	A-FER-FERR-211122/235
Vendor: Flatcore					
Product: flatcore-cms					
Affected Version(s): 2.1.0					
Improper Neutralization of Input During Web Page Generation	09-Nov-2022	6.1	A cross-site scripting (XSS) vulnerability in flatCore-CMS v2.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected	N/A	A-FLA-FLAT-211122/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			into the Username text field. **CVE ID : CVE-2022-43118**		
Vendor: flowring					
Product: agentflow					
Affected Version(s): 4.0.0.1183.552					
Unrestricted Upload of File with Dangerous Type	10-Nov-2022	9.8	The file upload function of Agentflow BPM has insufficient filtering for special characters in URLs. An unauthenticated remote attacker can exploit this vulnerability to upload arbitrary file and execute arbitrary code to manipulate system or disrupt service. **CVE ID : CVE-2022-39036**	https://www.flowring.com/2022/09/19/%e7%94%a2%e5%93%81%e6%9b%b4%e6%96%b0agentflow-v4-0%e3%80%81v3-7%e5%a4%be%e6%aa%94%e5%8a%9f%e8%83%bd%e8%b3%87%e5%ae%89%e4%bf%ae%e6%ad%a3/	A-FLO-AGEN-211122/237
Improper Authentication	10-Nov-2022	8.8	Agentflow BPM enterprise management system has improper authentication. A remote attacker with general user privilege can change the name of the user account to acquire arbitrary account privilege, and access, manipulate system or disrupt service.	https://www.flowring.com/2022/09/19/%e7%94%a2%e5%93%81%e6%9b%b4%e6%96%b0agentflow-v4-0%e3%80%81v3-7%e5%a4%be%e6%aa%94%e5%8a%9f%e8%83%bd%e8%b3%87%e5%ae%89	A-FLO-AGEN-211122/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39038	%e4%bf%ae%e6%ad%a3/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Nov-2022	7.5	Agentflow BPM file download function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and download arbitrary system files. **CVE ID : CVE-2022-39037**	https://www.flowring.com/2022/09/19/%e7%94%a2%e5%93%81%e6%9b%b4%e6%96%b0agentflow-v4-0%e3%80%81v3-7%e5%a4%be%e6%aa%94%e5%8a%9f%e8%83%bd%e8%b3%87%e5%ae%89%e4%bf%ae%e6%ad%a3/	A-FLO-AGEN-211122/239
Vendor: fluentd					
Product: fluentd					
Affected Version(s): From (including) 1.13.2 Up to (excluding) 1.15.3					
Deserialization of Untrusted Data	02-Nov-2022	9.8	Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. A remote code execution (RCE) vulnerability in non-default configurations of Fluentd allows unauthenticated attackers to execute arbitrary code via specially crafted JSON payloads.	https://github.com/fluent/fluentd/commit/48e5b85dab1b6d4c273090d538fc11b3f2fd8135, https://github.com/fluent/fluentd/security/advisories/GHSA-fppq-mj76-fpj2	A-FLU-FLUE-211122/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fluentd setups are only affected if the environment variable `FLUENT_OJ_OPTION_MODE` is explicitly set to `object`. Please note: The option FLUENT_OJ_OPTION_MODE was introduced in Fluentd version 1.13.2. Earlier versions of Fluentd are not affected by this vulnerability. This issue was patched in version 1.15.3. As a workaround do not use `FLUENT_OJ_OPTION_MODE=object`. **CVE ID : CVE-2022-39379**		
Vendor: fluentforms					
Product: contact_form					
Affected Version(s): * Up to (excluding) 4.3.13					
Improper Neutralization of Formula Elements in a CSV File	07-Nov-2022	9.8	The Contact Form Plugin WordPress plugin before 4.3.13 does not validate and escape fields when exporting form entries as CSV, leading to a CSV injection **CVE ID : CVE-2022-3463**	https://wpscan.com/vulnerability/e2a59481-db45-4b8e-b17a-447303469364	A-FLU-CONT-211122/241
Vendor: follow_me_plugin_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: follow_me_plugin					
Affected Version(s): * Up to (including) 3.1.1					
Cross-Site Request Forgery (CSRF)	15-Nov-2022	8.8	The "Follow Me Plugin" plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.1.1. This is due to missing nonce validation on the FollowMeIgniteSocialMedia_options_page() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious JavaScript via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2022-3240**	N/A	A-FOL-FOLL-211122/242
Vendor: food_ordering_management_system_project					
Product: food_ordering_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	07-Nov-2022	7.2	Food Ordering Management System v1.0 was discovered to contain a SQL injection vulnerability via the component	N/A	A-FOO-FOOD-211122/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			/foms/all-orders.php?status=Cancelled%20by%20Customer. **CVE ID : CVE-2022-42990**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Nov-2022	4.8	Food Ordering Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /foms/place-order.php. **CVE ID : CVE-2022-43046**	N/A	A-FOO-FOOD-211122/244
Vendor: Fortinet					
Product: antivirus_engine					
Affected Version(s): 0.4.23					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.0.49					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/246
Affected Version(s): 2.0.60					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 4.4.54					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/248
Affected Version(s): 6.137					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.142					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/250
Affected Version(s): 6.144					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.145					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/252
Affected Version(s): 6.156					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.157					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/254
Affected Version(s): 6.243					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.252					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/256
Affected Version(s): 6.253					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.33					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-ANTI-211122/258
Product: fortiadc					
Affected Version(s): 7.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiADC management interface 7.1.0 may allow a remote and authenticated attacker to trigger a stored cross site scripting (XSS) attack via configuring a specially crafted IP Address. **CVE ID : CVE-2022-35851**	https://fortiguard.com/psirt/FG-IR-22-314	A-FOR-FORT-211122/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 5.0.0 Up to (including) 5.0.4					
N/A	02-Nov-2022	9.8	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0 through 6.2.3, and 7.0.0 through 7.0.2. This may allow a remote attacker without privileges to bypass some Web Application Firewall (WAF) protection such as the SQL Injection and XSS filters via a malformed HTTP request. **CVE ID : CVE-2022-38381**	https://fortiguard.com/psirt/FG-IR-22-234	A-FOR-FORT-211122/260
Affected Version(s): From (including) 5.1.0 Up to (including) 5.1.7					
N/A	02-Nov-2022	9.8	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0 through 6.2.3, and 7.0.0 through 7.0.2. This may allow a remote attacker without privileges to bypass some Web Application Firewall (WAF)	https://fortiguard.com/psirt/FG-IR-22-234	A-FOR-FORT-211122/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection such as the SQL Injection and XSS filters via a malformed HTTP request. **CVE ID : CVE-2022-38381**		
Affected Version(s): From (including) 5.2.0 Up to (including) 5.2.8					
N/A	02-Nov-2022	9.8	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0 through 6.2.3, and 7.0.0 through 7.0.2. This may allow a remote attacker without privileges to bypass some Web Application Firewall (WAF) protection such as the SQL Injection and XSS filters via a malformed HTTP request. **CVE ID : CVE-2022-38381**	https://fortiguard.com/psirt/FG-IR-22-234	A-FOR-FORT-211122/262
Affected Version(s): From (including) 5.3.0 Up to (including) 5.3.7					
N/A	02-Nov-2022	9.8	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0	https://fortiguard.com/psirt/FG-IR-22-234	A-FOR-FORT-211122/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 6.2.3, and 7.0.0 through 7.0.2. This may allow a remote attacker without privileges to bypass some Web Application Firewall (WAF) protection such as the SQL Injection and XSS filters via a malformed HTTP request. **CVE ID : CVE-2022-38381**		
Affected Version(s): From (including) 5.4.0 Up to (including) 5.4.5					
N/A	02-Nov-2022	9.8	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0 through 6.2.3, and 7.0.0 through 7.0.2. This may allow a remote attacker without privileges to bypass some Web Application Firewall (WAF) protection such as the SQL Injection and XSS filters via a malformed HTTP request. **CVE ID : CVE-2022-38381**	https://fortiguard.com/psirt/FG-IR-22-234	A-FOR-FORT-211122/264
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Nov-2022	9.8	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0 through 6.2.3, and 7.0.0 through 7.0.2. This may allow a remote attacker without privileges to bypass some Web Application Firewall (WAF) protection such as the SQL Injection and XSS filters via a malformed HTTP request. **CVE ID : CVE-2022-38381**	https://fortiguard.com/psirt/FG-IR-22-234	A-FOR-FORT-211122/265
Affected Version(s): From (including) 6.1.0 Up to (including) 6.1.6					
N/A	02-Nov-2022	9.8	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0 through 6.2.3, and 7.0.0 through 7.0.2. This may allow a remote attacker without privileges to bypass some Web Application Firewall (WAF) protection such as	https://fortiguard.com/psirt/FG-IR-22-234	A-FOR-FORT-211122/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the SQL Injection and XSS filters via a malformed HTTP request. **CVE ID : CVE-2022-38381**		
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	6.1	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiADC 7.0.0 - 7.0.2 and 6.2.0 - 6.2.4 allows an attacker to execute unauthorized code or commands via the URL and User fields observed in the traffic and event logviews. **CVE ID : CVE-2022-38374**	https://fortiguard.com/psirt/FG-IR-22-232	A-FOR-FORT-211122/267
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.3					
N/A	02-Nov-2022	9.8	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0 through 6.2.3, and 7.0.0 through 7.0.2. This may allow a remote attacker without privileges to bypass some	https://fortiguard.com/psirt/FG-IR-22-234	A-FOR-FORT-211122/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Web Application Firewall (WAF) protection such as the SQL Injection and XSS filters via a malformed HTTP request. **CVE ID : CVE-2022-38381**		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	6.1	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiADC 7.0.0 - 7.0.2 and 6.2.0 - 6.2.4 allows an attacker to execute unauthorized code or commands via the URL and User fields observed in the traffic and event logviews. **CVE ID : CVE-2022-38374**	https://fortiguard.com/psirt/FG-IR-22-232	A-FOR-FORT-211122/269
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.2					
N/A	02-Nov-2022	9.8	An improper handling of malformed request vulnerability [CWE-228] exists in FortiADC 5.0 all versions, 6.0.0 all versions, 6.1.0 all versions, 6.2.0 through 6.2.3, and 7.0.0 through 7.0.2. This may allow a	https://fortiguard.com/psirt/FG-IR-22-234	A-FOR-FORT-211122/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker without privileges to bypass some Web Application Firewall (WAF) protection such as the SQL Injection and XSS filters via a malformed HTTP request. **CVE ID : CVE-2022-38381**		
Product: fortianalyzer					
Affected Version(s): From (including) 6.0.0 Up to (including) 6.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] exists in FortiManager and FortiAnalyzer 6.0.0 all versions, 6.2.0 all versions, 6.4.0 through 6.4.8, and 7.0.0 through 7.0.4. Report templates may allow a low privilege level attacker to perform an XSS attack via posting a crafted CKeditor "protected" comment as described in CVE-2020-9281. **CVE ID : CVE-2022-39950**	https://fortiguard.com/psirt/FG-IR-21-228	A-FOR-FORT-211122/271
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] exists in FortiManager and FortiAnalyzer 6.0.0 all versions, 6.2.0 all versions, 6.4.0 through 6.4.8, and 7.0.0 through 7.0.4. Report templates may allow a low privilege level attacker to perform an XSS attack via posting a crafted CKeditor "protected" comment as described in CVE-2020-9281. **CVE ID : CVE-2022-39950**	https://fortiguard.com/psirt/FG-IR-21-228	A-FOR-FORT-211122/272
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] exists in FortiManager and FortiAnalyzer 6.0.0 all versions, 6.2.0 all versions, 6.4.0 through 6.4.8, and 7.0.0 through 7.0.4. Report templates may allow a low privilege level attacker to perform an XSS attack via	https://fortiguard.com/psirt/FG-IR-21-228	A-FOR-FORT-211122/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			posting a crafted CKeditor "protected" comment as described in CVE-2020-9281. **CVE ID : CVE-2022-39950**		
Product: forticlient					
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.5					
Insertion of Sensitive Information into Log File	02-Nov-2022	5.5	An exposure of sensitive information to an unauthorized actor vulnerabiltiy [CWE-200] in FortiClient for Mac versions 7.0.0 through 7.0.5 may allow a local authenticated attacker to obtain the SSL-VPN password in cleartext via running a logstream for the FortiTray process in the terminal. **CVE ID : CVE-2022-33878**	https://fortiguard.com/psirt/FG-IR-22-246	A-FOR-FORT-211122/274
Product: fortideceptor					
Affected Version(s): 4.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiDeceptor management interface 4.2.0,	https://fortiguard.com/psirt/FG-IR-22-331	A-FOR-FORT-211122/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.1.0 through 4.1.1, 4.0.2 may allow an authenticated user to perform a cross site scripting (XSS) attack via sending requests with specially crafted lure resource ID. **CVE ID : CVE-2022-38373**		
Affected Version(s): 4.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiDeceptor management interface 4.2.0, 4.1.0 through 4.1.1, 4.0.2 may allow an authenticated user to perform a cross site scripting (XSS) attack via sending requests with specially crafted lure resource ID. **CVE ID : CVE-2022-38373**	https://fortiguard.com/psirt/FG-IR-22-331	A-FOR-FORT-211122/276
Affected Version(s): 4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiDeceptor management interface 4.2.0,	https://fortiguard.com/psirt/FG-IR-22-331	A-FOR-FORT-211122/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.1.0 through 4.1.1, 4.0.2 may allow an authenticated user to perform a cross site scripting (XSS) attack via sending requests with specially crafted lure resource ID. **CVE ID : CVE-2022-38373**		
Affected Version(s): 4.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiDeceptor management interface 4.2.0, 4.1.0 through 4.1.1, 4.0.2 may allow an authenticated user to perform a cross site scripting (XSS) attack via sending requests with specially crafted lure resource ID. **CVE ID : CVE-2022-38373**	https://fortiguard.com/psirt/FG-IR-22-331	A-FOR-FORT-211122/278
Product: fortiedr					
Affected Version(s): From (including) 4.0.0 Up to (including) 4.1.0					
Improper Resource Shutdown or Release	02-Nov-2022	5.5	An improper control of a resource through its lifetime vulnerability [CWE-664] in FortiEDR CollectorWindows 4.0.0 through 4.1,	https://fortiguard.com/psirt/FG-IR-22-218	A-FOR-FORT-211122/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.0.0 through 5.0.3.751, 5.1.0 may allow a privileged user to terminate the FortiEDR processes with special tools and bypass the EDR protection. **CVE ID : CVE-2022-39949**		
Affected Version(s): From (including) 5.0.0 Up to (including) 5.0.3.751					
Improper Resource Shutdown or Release	02-Nov-2022	5.5	An improper control of a resource through its lifetime vulnerability [CWE-664] in FortiEDR CollectorWindows 4.0.0 through 4.1, 5.0.0 through 5.0.3.751, 5.1.0 may allow a privileged user to terminate the FortiEDR processes with special tools and bypass the EDR protection. **CVE ID : CVE-2022-39949**	https://fortiguard.com/psirt/FG-IR-22-218	A-FOR-FORT-211122/280
Affected Version(s): From (including) 5.1.0 Up to (including) 5.2.0.2288					
Improper Resource Shutdown or Release	02-Nov-2022	5.5	An improper control of a resource through its lifetime vulnerability [CWE-664] in FortiEDR CollectorWindows 4.0.0 through 4.1, 5.0.0 through 5.0.3.751, 5.1.0 may	https://fortiguard.com/psirt/FG-IR-22-218	A-FOR-FORT-211122/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a privileged user to terminate the FortiEDR processes with special tools and bypass the EDR protection. **CVE ID : CVE-2022-39949**		
Product: fortimail					
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.2					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-FORT-211122/282
Affected Version(s): 4.1.0					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-FORT-211122/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**		
Affected Version(s): 7.2.0					
Authorization Bypass Through User-Controlled Key	02-Nov-2022	6.5	An improper access control vulnerability [CWE-284] in FortiMail 7.2.0, 7.0.0 through 7.0.3, 6.4 all versions, 6.2 all versions, 6.0 all versions may allow an authenticated admin user assigned to a specific domain to access and modify other domains information via insecure direct object references (IDOR). **CVE ID : CVE-2022-39945**	https://fortiguard.com/psirt/FG-IR-22-066	A-FOR-FORT-211122/284
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.12					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-FORT-211122/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**		
Authorization Bypass Through User-Controlled Key	02-Nov-2022	6.5	An improper access control vulnerability [CWE-284] in FortiMail 7.2.0, 7.0.0 through 7.0.3, 6.4 all versions, 6.2 all versions, 6.0 all versions may allow an authenticated admin user assigned to a specific domain to access and modify other domains information via insecure direct object references (IDOR). **CVE ID : CVE-2022-39945**	https://fortiguard.com/psirt/FG-IR-22-066	A-FOR-FORT-211122/286
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.9					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-FORT-211122/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**		
Authorization Bypass Through User-Controlled Key	02-Nov-2022	6.5	An improper access control vulnerability [CWE-284] in FortiMail 7.2.0, 7.0.0 through 7.0.3, 6.4 all versions, 6.2 all versions, 6.0 all versions may allow an authenticated admin user assigned to a specific domain to access and modify other domains information via insecure direct object references (IDOR). **CVE ID : CVE-2022-39945**	https://fortiguard.com/psirt/FG-IR-22-066	A-FOR-FORT-211122/288
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.6					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version	https://fortiguard.com/psirt/FG-IR-22-074	A-FOR-FORT-211122/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**		
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.7					
Authorization Bypass Through User-Controlled Key	02-Nov-2022	6.5	An improper access control vulnerability [CWE-284] in FortiMail 7.2.0, 7.0.0 through 7.0.3, 6.4 all versions, 6.2 all versions, 6.0 all versions may allow an authenticated admin user assigned to a specific domain to access and modify other domains information via insecure direct object references (IDOR). **CVE ID : CVE-2022-39945**	https://fortiguard.com/psirt/FG-IR-22-066	A-FOR-FORT-211122/290
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.3					
Authorization Bypass Through User-Controlled Key	02-Nov-2022	6.5	An improper access control vulnerability [CWE-284] in FortiMail 7.2.0, 7.0.0 through 7.0.3, 6.4 all versions, 6.2 all versions, 6.0 all	https://fortiguard.com/psirt/FG-IR-22-066	A-FOR-FORT-211122/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions may allow an authenticated admin user assigned to a specific domain to access and modify other domains information via insecure direct object references (IDOR). **CVE ID : CVE-2022-39945**		
Product: fortimanager					
Affected Version(s): From (including) 6.0.0 Up to (including) 6.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] exists in FortiManager and FortiAnalyzer 6.0.0 all versions, 6.2.0 all versions, 6.4.0 through 6.4.8, and 7.0.0 through 7.0.4. Report templates may allow a low privilege level attacker to perform an XSS attack via posting a crafted CKeditor "protected" comment as described in CVE-2020-9281. **CVE ID : CVE-2022-39950**	https://fortiguard.com/psirt/FG-IR-21-228	A-FOR-FORT-211122/292
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] exists in FortiManager and FortiAnalyzer 6.0.0 all versions, 6.2.0 all versions, 6.4.0 through 6.4.8, and 7.0.0 through 7.0.4. Report templates may allow a low privilege level attacker to perform an XSS attack via posting a crafted CKeditor "protected" comment as described in CVE-2020-9281. **CVE ID : CVE-2022-39950**	https://fortiguard.com/psirt/FG-IR-21-228	A-FOR-FORT-211122/293
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	An improper neutralization of input during web page generation vulnerability [CWE-79] exists in FortiManager and FortiAnalyzer 6.0.0 all versions, 6.2.0 all versions, 6.4.0 through 6.4.8, and 7.0.0 through 7.0.4. Report templates may allow a low privilege level attacker to perform an XSS attack via	https://fortiguard.com/psirt/FG-IR-21-228	A-FOR-FORT-211122/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			posting a crafted CKeditor "protected" comment as described in CVE-2020-9281. **CVE ID : CVE-2022-39950**		
Product: fortisiem					
Affected Version(s): 6.2.0					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/295
Affected Version(s): 5.0.0					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/296
Affected Version(s): 5.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/297
Affected Version(s): 5.2.1					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/298
Affected Version(s): 5.2.2					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password.	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26119		
Affected Version(s): 5.4.0					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/300
Affected Version(s): 6.2.1					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/301
Affected Version(s): 6.4.0					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**		
Affected Version(s): 6.4.1					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/303
Affected Version(s): From (including) 5.1.0 Up to (including) 5.1.3					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/304
Affected Version(s): From (including) 5.2.5 Up to (including) 5.2.8					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**		
Affected Version(s): From (including) 5.3.0 Up to (including) 5.3.3					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/306
Affected Version(s): From (including) 6.1.0 Up to (including) 6.1.2					
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/307
Affected Version(s): From (including) 6.3.0 Up to (including) 6.3.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	02-Nov-2022	7.8	A improper authentication vulnerability in Fortinet FortiSIEM before 6.5.0 allows a local attacker with CLI access to perform operations on the Glassfish server directly via a hardcoded password. **CVE ID : CVE-2022-26119**	https://fortiguard.com/psirt/FG-IR-22-064	A-FOR-FORT-211122/308
Product: fortisoar					
Affected Version(s): 7.2.0					
Missing Authentication for Critical Function	02-Nov-2022	5.5	A missing authentication for a critical function vulnerability in Fortinet FortiSOAR 6.4.0 - 6.4.4 and 7.0.0 - 7.0.3 and 7.2.0 allows an attacker to disclose information via logging into the database using a privileged account without a password. **CVE ID : CVE-2022-42473**	https://fortiguard.com/psirt/FG-IR-22-216	A-FOR-FORT-211122/309
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.3					
Missing Authentication for Critical Function	02-Nov-2022	5.5	A missing authentication for a critical function vulnerability in Fortinet FortiSOAR 6.4.0 - 6.4.4 and 7.0.0 - 7.0.3 and 7.2.0 allows an	https://fortiguard.com/psirt/FG-IR-22-216	A-FOR-FORT-211122/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose information via logging into the database using a privileged account without a password. **CVE ID : CVE-2022-42473**		
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.4					
Missing Authentication for Critical Function	02-Nov-2022	5.5	A missing authentication for a critical function vulnerability in Fortinet FortiSOAR 6.4.0 - 6.4.4 and 7.0.0 - 7.0.3 and 7.2.0 allows an attacker to disclose information via logging into the database using a privileged account without a password. **CVE ID : CVE-2022-42473**	https://fortiguard.com/psirt/FG-IR-22-216	A-FOR-FORT-211122/311
Product: fortitester					
Affected Version(s): 3.3.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**		
Affected Version(s): 7.0.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/313
N/A	02-Nov-2022	6.7	A hidden functionality vulnerability [CWE-1242] in FortiTester CLI 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0	https://fortiguard.com/psirt/FG-IR-22-283	A-FOR-FORT-211122/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a local, privileged user to obtain a root shell on the device via an undocumented command. **CVE ID : CVE-2022-38372**		
Affected Version(s): 7.1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/315
N/A	02-Nov-2022	6.7	A hidden functionality vulnerability [CWE-1242] in FortiTester CLI 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow a local, privileged user to	https://fortiguard.com/psirt/FG-IR-22-283	A-FOR-FORT-211122/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain a root shell on the device via an undocumented command. **CVE ID : CVE-2022-38372**		
Affected Version(s): 3.0.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/317
Affected Version(s): 4.1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**		
Affected Version(s): 4.1.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/319
Affected Version(s): 4.2.0					
Improper Neutralization of Special Elements	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**		
Affected Version(s): 3.1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 3.2.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/322
Affected Version(s): 3.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**		
Affected Version(s): 3.4.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/324
Affected Version(s): 3.5.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**		
Affected Version(s): 3.5.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/326
Affected Version(s): 3.6.0					
Improper Neutralization of Special Elements used in an	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**		
Affected Version(s): 3.7.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/328
Affected Version(s): 3.7.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/329
Affected Version(s): 3.8.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments to existing commands. **CVE ID : CVE-2022-33870**		
Affected Version(s): 3.9.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/331
Affected Version(s): 3.9.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**		
Affected Version(s): 4.0.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Nov-2022	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 3.0.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2022-33870**	https://fortiguard.com/psirt/FG-IR-22-070	A-FOR-FORT-211122/333
Affected Version(s): From (including) 2.3.0 Up to (including) 3.9.1					
N/A	02-Nov-2022	6.7	A hidden functionality vulnerability [CWE-1242] in FortiTester CLI 2.3.0 through 3.9.1, 4.0.0 through 4.2.0,	https://fortiguard.com/psirt/FG-IR-22-283	A-FOR-FORT-211122/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.0.0 through 7.1.0 may allow a local, privileged user to obtain a root shell on the device via an undocumented command. **CVE ID : CVE-2022-38372**		
Affected Version(s): From (including) 4.0.0 Up to (including) 4.2.0					
N/A	02-Nov-2022	6.7	A hidden functionality vulnerability [CWE-1242] in FortiTester CLI 2.3.0 through 3.9.1, 4.0.0 through 4.2.0, 7.0.0 through 7.1.0 may allow a local, privileged user to obtain a root shell on the device via an undocumented command. **CVE ID : CVE-2022-38372**	https://fortiguard.com/psirt/FG-IR-22-283	A-FOR-FORT-211122/335
Vendor: foru_cms_project					
Product: foru_cms					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	5.4	A vulnerability was found in ForU CMS. It has been classified as problematic. Affected is an unknown function of the file cms_chip.php. The manipulation of the argument name leads to cross site	N/A	A-FOR-FORU-211122/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-213450 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3943**		
Vendor: Foxitsoftware					
Product: foxit_reader					
Affected Version(s): * Up to (excluding) 11.2.118.51569					
Uncontrolled Search Path Element	09-Nov-2022	7.8	An Uncontrolled Search Path Element in Foxit Software released Foxit Reader v11.2.118.51569 allows attackers to escalate privileges when searching for DLL libraries without specifying an absolute path. **CVE ID : CVE-2022-43310**	https://www.foxitsoftware.com/support/security-bulletins.php, https://www.foxitsoftware.cn/support/security-bulletins.html	A-FOX-FOXI-211122/337
Vendor: frappe					
Product: frappe					
Affected Version(s): * Up to (including) 14.14.3					
Improper Neutralization of Input During Web Page Generation	14-Nov-2022	6.1	A vulnerability was found in Frappe. It has been rated as problematic. Affected by this issue is some unknown functionality of the	https://github.com/frappe/frappe/commit/bfab7191543961c6cb77fe267063877c31b616ce, https://github	A-FRA-FRAP-211122/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			file frappe/templates/includes/navbar/navbar_search.html of the component Search. The manipulation of the argument q leads to cross site scripting. The attack may be launched remotely. The name of the patch is bfab7191543961c6cb77fe267063877c31b616ce. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-213560. **CVE ID : CVE-2022-3988**	.com/frappe/frappe/pull/18847	
Vendor: frauscher					
Product: frauscher_diagnostic_system_102					
Affected Version(s): 2.9.0					
Unrestricted Upload of File with Dangerous Type	02-Nov-2022	9.8	Frauscher Sensortechnik GmbH FDS102 for FAdC R2 and FAdCi R2 v2.8.0 to v2.9.1 are vulnerable to malicious code upload without authentication by using the configuration upload function. This could lead to a complete	https://www.frauscher.com/en/psirt	A-FRA-FRAU-211122/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise of the FDS102 device. **CVE ID : CVE-2022-3575**		
Affected Version(s): 2.8.0					
Unrestricted Upload of File with Dangerous Type	02-Nov-2022	9.8	Frauscher Sensortechnik GmbH FDS102 for FAdC R2 and FAdCi R2 v2.8.0 to v2.9.1 are vulnerable to malicious code upload without authentication by using the configuration upload function. This could lead to a complete compromise of the FDS102 device. **CVE ID : CVE-2022-3575**	https://www.frauscher.com/en/psirt	A-FRA-FRAU-211122/340
Affected Version(s): 2.9.1					
Unrestricted Upload of File with Dangerous Type	02-Nov-2022	9.8	Frauscher Sensortechnik GmbH FDS102 for FAdC R2 and FAdCi R2 v2.8.0 to v2.9.1 are vulnerable to malicious code upload without authentication by using the configuration upload function. This could lead to a complete compromise of the FDS102 device.	https://www.frauscher.com/en/psirt	A-FRA-FRAU-211122/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3575		
Vendor: Froxlor					
Product: froxlor					
Affected Version(s): * Up to (excluding) 0.10.38.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Nov-2022	6.1	Code Injection in GitHub repository froxlor/froxlor prior to 0.10.38.2. **CVE ID : CVE-2022-3869**	https://huntr.dev/bounties/7de20f21-4a9b-445d-ae2b-15ade648900b, https://github.com/froxlor/froxlor/commit/3f10a4adede9df83408d60ded78b51b812a763a8	A-FRO-FROX-211122/342
Affected Version(s): * Up to (excluding) 0.10.39					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	4.6	Code Injection in GitHub repository froxlor/froxlor prior to 0.10.39. **CVE ID : CVE-2022-3721**	https://github.com/froxlor/froxlor/commit/1182453c18a83309a3470b2775c148ede740806c, https://huntr.dev/bounties/a3c506f0-5f8a-4eaa-b8cc-46fb9e35cf7a	A-FRO-FROX-211122/343
Vendor: garage_management_system_project					
Product: garage_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	02-Nov-2022	7.2	Garage Management System v1.0 was discovered to	N/A	A-GAR-GARA-211122/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			contain a SQL injection vulnerability via the id parameter at /garage/editorder.php. **CVE ID : CVE-2022-41551**		
Vendor: getshortcodes					
Product: shortcodes_ultimate					
Affected Version(s): * Up to (including) 5.12.0					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability leading to Stored Cross-Site Scripting (XSS) in Vladimir Anokhin's Shortcodes Ultimate plugin <= 5.12.0 on WordPress. **CVE ID : CVE-2022-41136**	https://patchstack.com/database/vulnerability/shortcodes-ultimate/wordpress-shortcodes-ultimate-plugin-5-12-0-csrf-vulnerability-leading-to-stored-xss?_s_id=cve, https://wordpress.org/plugins/shortcodes-ultimate/#developers	A-GET-SHOR-211122/345
Vendor: gifdec_project					
Product: gifdec					
Affected Version(s): -					
Out-of-bounds Read	07-Nov-2022	7.8	Gifdec commit 1dcbae19363597314f6623010cc80abad4e47f7c was discovered to contain an out-of-	https://github.com/lecram/gifdec/pull/23	A-GIF-GIFD-211122/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds read in the function read_image_data. This vulnerability is triggered when parsing a crafted Gif file. **CVE ID : CVE-2022-43359**		
Vendor: Github					
Product: enterprise_server					
Affected Version(s): From (including) 3.2.0 Up to (excluding) 3.2.20					
Files or Directories Accessible to External Parties	01-Nov-2022	5.7	An improper cache key vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to access private repository files through a public repository. To exploit this, an actor would need to already be authorized on the GitHub Enterprise Server instance, be able to create a public repository, and have a site administrator visit a specially crafted URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, 3.6.3.	https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.20, https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.10	A-GIT-ENTE-211122/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23738**		
Affected Version(s): From (including) 3.3.0 Up to (excluding) 3.3.15					
Files or Directories Accessible to External Parties	01-Nov-2022	5.7	An improper cache key vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to access private repository files through a public repository. To exploit this, an actor would need to already be authorized on the GitHub Enterprise Server instance, be able to create a public repository, and have a site administrator visit a specially crafted URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program.	https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.20, https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.10	A-GIT-ENTE-211122/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23738		
Affected Version(s): From (including) 3.4.0 Up to (excluding) 3.4.10					
Files or Directories Accessible to External Parties	01-Nov-2022	5.7	An improper cache key vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to access private repository files through a public repository. To exploit this, an actor would need to already be authorized on the GitHub Enterprise Server instance, be able to create a public repository, and have a site administrator visit a specially crafted URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23738**	https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.20, https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.10	A-GIT-ENTE-211122/349
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.7					
Files or Directories	01-Nov-2022	5.7	An improper cache key vulnerability	https://docs.github.com/en	A-GIT-ENTE-211122/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Accessible to External Parties			was identified in GitHub Enterprise Server that allowed an unauthorized actor to access private repository files through a public repository. To exploit this, an actor would need to already be authorized on the GitHub Enterprise Server instance, be able to create a public repository, and have a site administrator visit a specially crafted URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23738**	/enterprise-server@3.2/admin/release-notes#3.2.20, https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.10	
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.3					
Files or Directories Accessible to External Parties	01-Nov-2022	5.7	An improper cache key vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to access private repository	https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.20, https://docs.github.com/en	A-GIT-ENTE-211122/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files through a public repository. To exploit this, an actor would need to already be authorized on the GitHub Enterprise Server instance, be able to create a public repository, and have a site administrator visit a specially crafted URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23738**	/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.10	
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): * Up to (excluding) 15.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2. It was possible to exploit a	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3265.json	A-GIT-GITL-211122/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in setting the labels colour feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side. **CVE ID : CVE-2022-3265**		
Uncontrolled Resource Consumption	10-Nov-2022	5.3	An uncontrolled resource consumption issue when parsing URLs in GitLab CE/EE affecting all versions prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to cause performance issues and potentially a denial of service on the GitLab instance. **CVE ID : CVE-2022-3818**	https://gitlab.com/gitlab-org/gitlab/-/issues/358170, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3818.json	A-GIT-GITL-211122/353
Affected Version(s): 15.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions starting from 15.2 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2904.json	A-GIT-GITL-211122/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 15.4 before 15.4.1 It was possible to exploit a vulnerability in the external status checks feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side. **CVE ID : CVE-2022-2904**		
Affected Version(s): 15.4.0					
N/A	09-Nov-2022	7.5	Bypass of healthcheck endpoint allow list affecting all versions from 12.0 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an unauthorized attacker to prevent access to GitLab **CVE ID : CVE-2022-3285**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3285.json, https://gitlab.com/gitlab-org/security/omnibus-gitlab/-/issues/64	A-GIT-GITL-211122/355
Affected Version(s): From (including) 10.1.0 Up to (excluding) 15.3.5					
URL Redirection to Untrusted Site ('Open Redirect')	09-Nov-2022	6.1	An open redirect in GitLab CE/EE affecting all versions from 10.1 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to trick users into visiting a trustworthy URL	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3280.json	A-GIT-GITL-211122/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and being redirected to arbitrary content. **CVE ID : CVE-2022-3280**		
Affected Version(s): From (including) 12.0.0 Up to (excluding) 15.2.5					
N/A	09-Nov-2022	7.5	Bypass of healthcheck endpoint allow list affecting all versions from 12.0 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an unauthorized attacker to prevent access to GitLab **CVE ID : CVE-2022-3285**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3285.json, https://gitlab.com/gitlab-org/security/omnibus-gitlab/-/issues/64	A-GIT-GITL-211122/357
Affected Version(s): From (including) 12.1.0 Up to (excluding) 15.3.5					
N/A	09-Nov-2022	5.4	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.1 before 15.3.5, all versions starting from 15.4 before 15.4.4, all versions starting from 15.5 before 15.5.2. A malicious maintainer could exfiltrate a Datadog integration's access token by modifying the integration URL such that authenticated requests are sent to	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3483.json	A-GIT-GITL-211122/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker controlled server. **CVE ID : CVE-2022-3483**		
Affected Version(s): From (including) 12.6.0 Up to (excluding) 15.3.5					
N/A	10-Nov-2022	9	Lack of sand-boxing of OpenAPI documents in GitLab CE/EE affecting all versions from 12.6 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to trick a user to click on the Swagger OpenAPI viewer and issue HTTP requests that affect the victim's account. **CVE ID : CVE-2022-3726**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3726.json, https://gitlab.com/gitlab-org/gitlab/-/issues/362509	A-GIT-GITL-211122/359
N/A	10-Nov-2022	5.3	An improper authorization issue in GitLab CE/EE affecting all versions from 14.4 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to read variables set directly in a GitLab CI/CD configuration file they don't have access to. **CVE ID : CVE-2022-3793**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3793.json, https://gitlab.com/gitlab-org/gitlab/-/issues/372120	A-GIT-GITL-211122/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 13.9.0 Up to (excluding) 15.3.5					
N/A	09-Nov-2022	5.3	An information disclosure issue in GitLab CE/EE affecting all versions from 14.4 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to use GitLab Flavored Markdown (GFM) references in a Jira issue to disclose the names of resources they don't have access to. **CVE ID : CVE-2022-2761**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2761.json	A-GIT-GITL-211122/361
Affected Version(s): From (including) 14.5.0 Up to (excluding) 15.3.5					
Incorrect Authorization	10-Nov-2022	4.3	Incorrect authorization during display of Audit Events in GitLab EE affecting all versions from 14.5 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2, allowed Developers to view the project's Audit Events and Developers or Maintainers to view the group's Audit Events. These should have been restricted to Project Maintainers, Group Owners, and above.	https://gitlab.com/gitlab-org/gitlab/-/issues/374926, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3413.json	A-GIT-GITL-211122/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3413		
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.3.5					
N/A	10-Nov-2022	4.3	An improper authorization issue in GitLab CE/EE affecting all versions from 15.0 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows a malicious users to set emojis on internal notes they don't have access to. **CVE ID : CVE-2022-3819**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3819.json, https://gitlab.com/gitlab-org/gitlab/-/issues/365847	A-GIT-GITL-211122/363
Affected Version(s): From (including) 15.2 Up to (excluding) 15.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions starting from 15.2 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 It was possible to exploit a vulnerability in the external status checks feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2904.json	A-GIT-GITL-211122/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behalf of victims at client side. **CVE ID : CVE-2022-2904**		
Affected Version(s): From (including) 15.2 Up to (including) 15.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions starting from 15.2 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 It was possible to exploit a vulnerability in the external status checks feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side. **CVE ID : CVE-2022-2904**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2904.json	A-GIT-GITL-211122/365
Affected Version(s): From (including) 15.3 Up to (excluding) 15.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions starting from 15.2 before 15.2.5, all versions starting from 15.3 before 15.3.4, all	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2904.json	A-GIT-GITL-211122/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions starting from 15.4 before 15.4.1 It was possible to exploit a vulnerability in the external status checks feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side. **CVE ID : CVE-2022-2904**		
Affected Version(s): From (including) 15.3 Up to (including) 15.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions starting from 15.2 before 15.2.5, all versions starting from 15.3 before 15.3.4, all versions starting from 15.4 before 15.4.1 It was possible to exploit a vulnerability in the external status checks feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2904.json	A-GIT-GITL-211122/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2904		
Affected Version(s): From (including) 15.3.0 Up to (excluding) 15.3.4					
N/A	09-Nov-2022	7.5	Bypass of healthcheck endpoint allow list affecting all versions from 12.0 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an unauthorized attacker to prevent access to GitLab **CVE ID : CVE-2022-3285**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3285.json, https://gitlab.com/gitlab-org/security/omnibus-gitlab/-/issues/64	A-GIT-GITL-211122/368
Affected Version(s): From (including) 15.4.0 Up to (excluding) 15.4.4					
N/A	10-Nov-2022	9	Lack of sand-boxing of OpenAPI documents in GitLab CE/EE affecting all versions from 12.6 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to trick a user to click on the Swagger OpenAPI viewer and issue HTTP requests that affect the victim's account. **CVE ID : CVE-2022-3726**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3726.json, https://gitlab.com/gitlab-org/gitlab/-/issues/362509	A-GIT-GITL-211122/369
URL Redirection to Untrusted	09-Nov-2022	6.1	An open redirect in GitLab CE/EE affecting all versions from 10.1 prior to 15.3.5, 15.4	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-	A-GIT-GITL-211122/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to trick users into visiting a trustworthy URL and being redirected to arbitrary content. **CVE ID : CVE-2022-3280**	2022-3280.json	
URL Redirection to Untrusted Site ('Open Redirect')	09-Nov-2022	6.1	An open redirect vulnerability in GitLab EE/CE affecting all versions from 9.3 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2, allows an attacker to redirect users to an arbitrary location if they trust the URL. **CVE ID : CVE-2022-3486**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3486.json	A-GIT-GITL-211122/371
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2. It was possible to exploit a vulnerability in setting the labels colour feature which could lead to a stored XSS that allowed attackers	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3265.json	A-GIT-GITL-211122/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to perform arbitrary actions on behalf of victims at client side. **CVE ID : CVE-2022-3265**		
N/A	09-Nov-2022	5.4	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.1 before 15.3.5, all versions starting from 15.4 before 15.4.4, all versions starting from 15.5 before 15.5.2. A malicious maintainer could exfiltrate a Datadog integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server. **CVE ID : CVE-2022-3483**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3483.json	A-GIT-GITL-211122/373
N/A	09-Nov-2022	5.3	An information disclosure issue in GitLab CE/EE affecting all versions from 14.4 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to use GitLab Flavored Markdown (GFM) references in a Jira	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2761.json	A-GIT-GITL-211122/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue to disclose the names of resources they don't have access to. **CVE ID : CVE-2022-2761**		
N/A	10-Nov-2022	5.3	An improper authorization issue in GitLab CE/EE affecting all versions from 14.4 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to read variables set directly in a GitLab CI/CD configuration file they don't have access to. **CVE ID : CVE-2022-3793**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3793.json, https://gitlab.com/gitlab-org/gitlab/-/issues/372120	A-GIT-GITL-211122/375
Uncontrolled Resource Consumption	10-Nov-2022	5.3	An uncontrolled resource consumption issue when parsing URLs in GitLab CE/EE affecting all versions prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to cause performance issues and potentially a denial of service on the GitLab instance. **CVE ID : CVE-2022-3818**	https://gitlab.com/gitlab-org/gitlab/-/issues/358170, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3818.json	A-GIT-GITL-211122/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	10-Nov-2022	4.3	Incorrect authorization during display of Audit Events in GitLab EE affecting all versions from 14.5 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2, allowed Developers to view the project's Audit Events and Developers or Maintainers to view the group's Audit Events. These should have been restricted to Project Maintainers, Group Owners, and above. **CVE ID : CVE-2022-3413**	https://gitlab.com/gitlab-org/gitlab/-/issues/374926, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3413.json	A-GIT-GITL-211122/377
N/A	10-Nov-2022	4.3	Improper authorization in GitLab CE/EE affecting all versions from 7.14 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows a user retrying a job in a downstream pipeline to take ownership of the retried jobs in the upstream pipeline even if the user doesn't have access to that project. **CVE ID : CVE-2022-3706**	https://gitlab.com/gitlab-org/gitlab/-/issues/365532, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3706.json	A-GIT-GITL-211122/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Nov-2022	4.3	An improper authorization issue in GitLab CE/EE affecting all versions from 15.0 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows a malicious users to set emojis on internal notes they don't have access to. **CVE ID : CVE-2022-3819**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3819.json, https://gitlab.com/gitlab-org/gitlab/-/issues/365847	A-GIT-GITL-211122/379
Affected Version(s): From (including) 15.5.0 Up to (excluding) 15.5.2					
N/A	10-Nov-2022	9	Lack of sand-boxing of OpenAPI documents in GitLab CE/EE affecting all versions from 12.6 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to trick a user to click on the Swagger OpenAPI viewer and issue HTTP requests that affect the victim's account. **CVE ID : CVE-2022-3726**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3726.json, https://gitlab.com/gitlab-org/gitlab/-/issues/362509	A-GIT-GITL-211122/380
URL Redirection to Untrusted Site ('Open Redirect')	09-Nov-2022	6.1	An open redirect in GitLab CE/EE affecting all versions from 10.1 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3280.json	A-GIT-GITL-211122/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an attacker to trick users into visiting a trustworthy URL and being redirected to arbitrary content. **CVE ID : CVE-2022-3280**		
URL Redirection to Untrusted Site ('Open Redirect')	09-Nov-2022	6.1	An open redirect vulnerability in GitLab EE/CE affecting all versions from 9.3 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2, allows an attacker to redirect users to an arbitrary location if they trust the URL. **CVE ID : CVE-2022-3486**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3486.json	A-GIT-GITL-211122/382
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2. It was possible to exploit a vulnerability in setting the labels colour feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3265.json	A-GIT-GITL-211122/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behalf of victims at client side. **CVE ID : CVE-2022-3265**		
N/A	09-Nov-2022	5.4	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.1 before 15.3.5, all versions starting from 15.4 before 15.4.4, all versions starting from 15.5 before 15.5.2. A malicious maintainer could exfiltrate a Datadog integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server. **CVE ID : CVE-2022-3483**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3483.json	A-GIT-GITL-211122/384
N/A	09-Nov-2022	5.3	An information disclosure issue in GitLab CE/EE affecting all versions from 14.4 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to use GitLab Flavored Markdown (GFM) references in a Jira issue to disclose the names of resources	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2761.json	A-GIT-GITL-211122/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they don't have access to. **CVE ID : CVE-2022-2761**		
N/A	10-Nov-2022	5.3	An improper authorization issue in GitLab CE/EE affecting all versions from 14.4 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to read variables set directly in a GitLab CI/CD configuration file they don't have access to. **CVE ID : CVE-2022-3793**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3793.json, https://gitlab.com/gitlab-org/gitlab/-/issues/372120	A-GIT-GITL-211122/386
Uncontrolled Resource Consumption	10-Nov-2022	5.3	An uncontrolled resource consumption issue when parsing URLs in GitLab CE/EE affecting all versions prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to cause performance issues and potentially a denial of service on the GitLab instance. **CVE ID : CVE-2022-3818**	https://gitlab.com/gitlab-org/gitlab/-/issues/358170, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3818.json	A-GIT-GITL-211122/387
Incorrect Authorization	10-Nov-2022	4.3	Incorrect authorization during display of	https://gitlab.com/gitlab-org/gitlab/-	A-GIT-GITL-211122/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Audit Events in GitLab EE affecting all versions from 14.5 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2, allowed Developers to view the project's Audit Events and Developers or Maintainers to view the group's Audit Events. These should have been restricted to Project Maintainers, Group Owners, and above. **CVE ID : CVE-2022-3413**	/issues/374926, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3413.json	
N/A	10-Nov-2022	4.3	Improper authorization in GitLab CE/EE affecting all versions from 7.14 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows a user retrying a job in a downstream pipeline to take ownership of the retried jobs in the upstream pipeline even if the user doesn't have access to that project. **CVE ID : CVE-2022-3706**	https://gitlab.com/gitlab-org/gitlab/-/issues/365532, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3706.json	A-GIT-GITL-211122/389
N/A	10-Nov-2022	4.3	An improper authorization issue in GitLab CE/EE	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-211122/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affecting all versions from 15.0 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows a malicious users to set emojis on internal notes they don't have access to. **CVE ID : CVE-2022-3819**	/blob/master/2022/CVE-2022-3819.json, https://gitlab.com/gitlab-org/gitlab/-/issues/365847	
Affected Version(s): From (including) 7.14.0 Up to (excluding) 15.3.5					
N/A	10-Nov-2022	4.3	Improper authorization in GitLab CE/EE affecting all versions from 7.14 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows a user retrying a job in a downstream pipeline to take ownership of the retried jobs in the upstream pipeline even if the user doesn't have access to that project. **CVE ID : CVE-2022-3706**	https://gitlab.com/gitlab-org/gitlab/-/issues/365532, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3706.json	A-GIT-GITL-211122/391
Affected Version(s): From (including) 9.4.0 Up to (excluding) 15.3.5					
URL Redirection to Untrusted Site ('Open Redirect')	09-Nov-2022	6.1	An open redirect vulnerability in GitLab EE/CE affecting all versions from 9.3 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2,	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3486.json	A-GIT-GITL-211122/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an attacker to redirect users to an arbitrary location if they trust the URL. **CVE ID : CVE-2022-3486**		
Vendor: Glpi-project					
Product: glpi					
Affected Version(s): * Up to (excluding) 10.0.4					
Insufficient Session Expiration	03-Nov-2022	8.8	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Deleted/deactivated user could continue to use their account as long as its cookie is valid. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds. **CVE ID : CVE-2022-39234**	https://github.com/glpi-project/glpi/security/advisories/GHSA-pgcx-mc58-3gmg	A-GLP-GLPI-211122/393
Server-Side Request Forgery (SSRF)	03-Nov-2022	5.3	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management	https://github.com/glpi-project/glpi/security/advisories/GHSA-	A-GLP-GLPI-211122/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Usage of RSS feeds or an external calendar in planning is subject to SSRF exploit. In case a remote script returns a redirect response, the redirect target URL is not checked against the URL allow list defined by administrator. This issue has been patched, please upgrade to 10.0.4. There are currently no known workarounds. **CVE ID : CVE-2022-39276**	8vwg-7x42-7v6p	
Affected Version(s): From (including) 0.60 Up to (excluding) 10.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	4.8	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. External links are not properly sanitized and can	https://github.com/glpi-project/glpi/security/advisories/GHSA-rhcw-8r7g-8pwc, https://huntr.dev/bounties/8e047ae1-7a7c-48e0-bee3-d1c36e52ff42/	A-GLP-GLPI-211122/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			therefore be used for a Cross-Site Scripting (XSS) attack. This issue has been patched, please upgrade to GLPI 10.0.4. There are currently no known workarounds. **CVE ID : CVE-2022-39277**		
Affected Version(s): From (including) 0.65 Up to (excluding) 10.0.4					
Improper Input Validation	03-Nov-2022	6.5	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Users may be able to inject custom fields values in `mailto` links. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds. **CVE ID : CVE-2022-39376**	https://github.com/glpi-project/glpi/security/advisories/GHSA-6rh5-m5g7-327w	A-GLP-GLPI-211122/396
Improper Neutralization of Input During	03-Nov-2022	4.8	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and	https://github.com/glpi-project/glpi/security/advisories/GHSA-	A-GLP-GLPI-211122/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			IT Management Software package, GLPI administrator can define rich-text content to be displayed on login page. The displayed content is can contains malicious code that can be used to steal credentials. This issue has been patched, please upgrade to version 10.0.4. **CVE ID : CVE-2022-39262**	4x48-q2wr-cpg4	
Affected Version(s): From (including) 0.70 Up to (excluding) 10.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Authenticated users may store malicious code in their account information. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds.	https://github.com/glpi-project/glpi/security/advisories/GHSA-5rj7-95qc-89h2	A-GLP-GLPI-211122/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39372		
Incorrect Authorization	03-Nov-2022	4.3	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Connected users may gain access to debug panel through the GLPI update script. This issue has been patched, please upgrade to 10.0.4. As a workaround, delete the `install/update.php` script. **CVE ID : CVE-2022-39370**	https://github.com/glpi-project/glpi/security/advisories/GHSA-6c2p-wgx9-vrjc	A-GLP-GLPI-211122/399
Affected Version(s): From (including) 0.84 Up to (excluding) 10.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Users may be able to create a public	https://github.com/glpi-project/glpi/security/advisories/GHSA-fxcx-93fq-8r9g	A-GLP-GLPI-211122/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RSS feed to inject malicious code in dashboards of other users. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds. **CVE ID : CVE-2022-39375**		
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Script related HTML tags in assets inventory information are not properly neutralized. This issue has been patched, please upgrade to version 10.0.4. There are currently no known workarounds. **CVE ID : CVE-2022-39371**	https://github.com/glpi-project/glpi/security/advisories/GHSA-w7wc-728f-6mm8	A-GLP-GLPI-211122/401
Improper Neutralization of	03-Nov-2022	4.8	GLPI stands for Gestionnaire Libre de Parc	https://github.com/glpi-project/glpi/s	A-GLP-GLPI-211122/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Administrator may store malicious code in entity name. This issue has been patched, please upgrade to version 10.0.4. **CVE ID : CVE-2022-39373**	ecurity/advisories/GHSA-cw37-q82c-w546	
Affected Version(s): From (including) 9.1 Up to (excluding) 10.0.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Nov-2022	9.8	GLPI stands for Gestionnaire Libre de Parc Informatique. GLPI is a Free Asset and IT Management Software package that provides ITIL Service Desk features, licenses tracking and software auditing. Time based attack using a SQL injection in api REST user_token. This issue has been patched, please upgrade to version 10.0.4. As a workaround, disable login with user_token on API Rest.	https://github.com/glpi-project/glpi/security/advisories/GHSA-cp6q-9p4x-8hr9	A-GLP-GLPI-211122/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39323		
Vendor: Golang					
Product: go					
Affected Version(s): * Up to (excluding) 1.18.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-Nov-2022	7.5	Due to unsanitized NUL values, attackers may be able to maliciously set environment variables on Windows. In syscall.StartProcess and os/exec.Cmd, invalid environment variable values containing NUL values are not properly checked for. A malicious environment variable value can exploit this behavior to set a value for a different environment variable. For example, the environment variable string "A=B\x00C=D" sets the variables "A=B" and "C=D". **CVE ID : CVE-2022-41716**	https://go.dev/cl/446916, https://pkg.go.dev/vuln/GO-2022-1095, https://go.dev/issue/56284, https://groups.google.com/g/golang-announce/c/mbHY1UY3BaM/m/hSpmRzk-AgAJ	A-GOL-GO-211122/404
Affected Version(s): From (including) 1.19.0 Up to (excluding) 1.19.3					
Improper Neutralization of Special Elements	02-Nov-2022	7.5	Due to unsanitized NUL values, attackers may be able to maliciously set environment	https://go.dev/cl/446916, https://pkg.go.dev/vuln/GO-2022-1095,	A-GOL-GO-211122/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in Output Used by a Downstream Component ('Injection')			variables on Windows. In syscall.StartProcess and os/exec.Cmd, invalid environment variable values containing NUL values are not properly checked for. A malicious environment variable value can exploit this behavior to set a value for a different environment variable. For example, the environment variable string "A=B\x00C=D" sets the variables "A=B" and "C=D". **CVE ID : CVE-2022-41716**	https://go.dev/issue/56284, https://groups.google.com/g/golang-announce/c/mbHY1UY3BaM/m/hSpmRzk-AgAJ	
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 106.0.5249.119					
Use After Free	09-Nov-2022	8.8	Use after free in Skia in Google Chrome prior to 106.0.5249.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	https://crbug.com/1364604, https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html	A-GOO-CHRO-211122/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3445		
Out-of-bounds Write	09-Nov-2022	8.8	Heap buffer overflow in WebSQL in Google Chrome prior to 106.0.5249.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3446**	https://crbug.com/1368076, https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html	A-GOO-CHRO-211122/407
Use After Free	09-Nov-2022	8.8	Use after free in Permissions API in Google Chrome prior to 106.0.5249.119 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3448**	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html	A-GOO-CHRO-211122/408
Use After Free	09-Nov-2022	8.8	Use after free in Safe Browsing in Google Chrome prior to 106.0.5249.119 allowed an attacker who convinced a	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.ht	A-GOO-CHRO-211122/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High) **CVE ID : CVE-2022-3449**	ml, https://crbug.com/1364662	
Use After Free	09-Nov-2022	8.8	Use after free in Peer Connection in Google Chrome prior to 106.0.5249.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3450**	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html, https://crbug.com/1369882	A-GOO-CHRO-211122/410
N/A	09-Nov-2022	4.3	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 106.0.5249.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: High)	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html	A-GOO-CHRO-211122/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3447		
Affected Version(s): * Up to (excluding) 106.0.5249.62					
Use After Free	01-Nov-2022	8.8	Use after free in CSS in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3304**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html, https://crbug.com/1358907	A-GOO-CHRO-211122/412
Use After Free	01-Nov-2022	8.8	Use after free in survey in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3305**	https://crbug.com/1319229, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	A-GOO-CHRO-211122/413
Use After Free	01-Nov-2022	8.8	Use after free in survey in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML	https://crbug.com/1320139, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-	A-GOO-CHRO-211122/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page. (Chromium security severity: High) **CVE ID : CVE-2022-3306**	desktop_27.html	
Use After Free	01-Nov-2022	8.8	Use after free in media in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3307**	https://crbug.com/1323488, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	A-GOO-CHRO-211122/415
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	8.8	Type confusion in Blink in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2022-3315**	https://crbug.com/1322812, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	A-GOO-CHRO-211122/416
N/A	01-Nov-2022	7.4	Insufficient policy enforcement in developer tools in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to potentially perform	https://crbug.com/1342722, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-	A-GOO-CHRO-211122/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a sandbox escape via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2022-3308**	desktop_27.html	
Use After Free	01-Nov-2022	6.5	Use after free in assistant in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via specific UI gestures. (Chromium security severity: Medium) **CVE ID : CVE-2022-3309**	https://crbug.com/1348415, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	A-GOO-CHRO-211122/418
N/A	01-Nov-2022	6.5	Insufficient policy enforcement in custom tabs in Google Chrome on Android prior to 106.0.5249.62 allowed an attacker who convinced the user to install an application to bypass same origin policy via a crafted application. (Chromium security severity: Medium)	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html, https://crbug.com/1240065	A-GOO-CHRO-211122/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3310		
Use After Free	01-Nov-2022	6.5	Use after free in import in Google Chrome prior to 106.0.5249.62 allowed a remote attacker who had compromised a WebUI process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2022-3311**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html, https://crbug.com/1302813	A-GOO-CHRO-211122/420
N/A	01-Nov-2022	6.5	Incorrect security UI in full screen in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2022-3313**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html, https://crbug.com/1317904	A-GOO-CHRO-211122/421
Use After Free	01-Nov-2022	6.5	Use after free in logging in Google Chrome prior to 106.0.5249.62 allowed a remote attacker who had compromised a WebUI process to potentially perform a sandbox escape	https://crbug.com/1328708, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-	A-GOO-CHRO-211122/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2022-3314**	desktop_27.html	
Use After Free	01-Nov-2022	6.5	Use after free in ChromeOS Notifications in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker who convinced a user to reboot Chrome OS to potentially exploit heap corruption via UI interaction. (Chromium security severity: Low) **CVE ID : CVE-2022-3318**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html, https://crbug.com/1318791	A-GOO-CHRO-211122/423
Improper Input Validation	01-Nov-2022	4.6	Insufficient validation of untrusted input in VPN in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a local attacker to bypass managed device restrictions via physical access to the device. (Chromium security severity: Medium)	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html, https://crbug.com/1303306	A-GOO-CHRO-211122/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3312		
Improper Input Validation	01-Nov-2022	4.3	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to bypass security feature via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2022-3316**	https://crbug.com/1333623, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	A-GOO-CHRO-211122/425
Improper Input Validation	01-Nov-2022	4.3	Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 106.0.5249.62 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2022-3317**	https://crbug.com/1300539, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	A-GOO-CHRO-211122/426
Improper Input Validation	01-Nov-2022	4.3	Insufficient data validation in File System API in Google Chrome prior to 106.0.5249.62 allowed a remote	https://crbug.com/1243802, https://chromereleases.googleblog.com/2022/09/stable-	A-GOO-CHRO-211122/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass File System restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2022-3443**	channel-update-for-desktop_27.html	
Improper Input Validation	01-Nov-2022	4.3	Insufficient data validation in File System API in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to bypass File System restrictions via a crafted HTML page and malicious file. (Chromium security severity: Low) **CVE ID : CVE-2022-3444**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html, https://crbug.com/1208439	A-GOO-CHRO-211122/428
Affected Version(s): * Up to (excluding) 106.0.5249.91					
Use After Free	01-Nov-2022	8.8	Use after free in Custom Elements in Google Chrome prior to 106.0.5249.91 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3370**	https://crbug.com/1366813	A-GOO-CHRO-211122/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Nov-2022	8.8	Out of bounds write in V8 in Google Chrome prior to 106.0.5249.91 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3373**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-211122/430
Affected Version(s): * Up to (excluding) 107.0.5304.106					
Out-of-bounds Write	09-Nov-2022	9.6	Heap buffer overflow in Crashpad in Google Chrome on Android prior to 107.0.5304.106 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3890**	https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html, https://crbug.com/1380083	A-GOO-CHRO-211122/431
Use After Free	09-Nov-2022	8.8	Use after free in V8 in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML	https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html	A-GOO-CHRO-211122/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page. (Chromium security severity: High) **CVE ID : CVE-2022-3885**		
Use After Free	09-Nov-2022	8.8	Use after free in Speech Recognition in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3886**	https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html, https://crbug.com/1372999	A-GOO-CHRO-211122/433
Use After Free	09-Nov-2022	8.8	Use after free in Web Workers in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3887**	https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html, https://crbug.com/1372695	A-GOO-CHRO-211122/434
Use After Free	09-Nov-2022	8.8	Use after free in WebCodecs in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to	https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html	A-GOO-CHRO-211122/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3888**		
Access of Resource Using Incompatible Type ('Type Confusion')	09-Nov-2022	8.8	Type confusion in V8 in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3889**	https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html	A-GOO-CHRO-211122/436
Affected Version(s): * Up to (excluding) 107.0.5304.62					
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	8.8	Type confusion in V8 in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3652**	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html, https://crbug.com/1369871	A-GOO-CHRO-211122/437
Out-of-bounds Write	01-Nov-2022	8.8	Heap buffer overflow in Vulkan in Google Chrome prior to 107.0.5304.62	https://chromereleases.googleblog.com/2022/10/stable-channel-	A-GOO-CHRO-211122/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3653**	update-for-desktop_25.html, https://crbug.com/1354271	
Use After Free	01-Nov-2022	8.8	Use after free in Layout in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3654**	https://crbug.com/1365330, https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-211122/439
Out-of-bounds Write	01-Nov-2022	8.8	Heap buffer overflow in Media Galleries in Google Chrome prior to 107.0.5304.62 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2022-3655**	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html, https://crbug.com/1343384	A-GOO-CHRO-211122/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	01-Nov-2022	8.8	Insufficient data validation in File System in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2022-3656**	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html, https://crbug.com/1345275	A-GOO-CHRO-211122/441
Use After Free	01-Nov-2022	8.8	Use after free in Extensions in Google Chrome prior to 107.0.5304.62 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Medium) **CVE ID : CVE-2022-3657**	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html, https://crbug.com/1351177	A-GOO-CHRO-211122/442
Use After Free	01-Nov-2022	8.8	Use after free in Feedback service on Chrome OS in Google Chrome on Chrome OS prior to 107.0.5304.62 allowed an attacker who convinced a user to install a	https://crbug.com/1352817, https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-	A-GOO-CHRO-211122/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious extension to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2022-3658**	desktop_25.html	
Use After Free	01-Nov-2022	8.8	Use after free in Accessibility in Google Chrome on Chrome OS prior to 107.0.5304.62 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via specific UI interactions. (Chromium security severity: Medium) **CVE ID : CVE-2022-3659**	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html, https://crbug.com/1355560	A-GOO-CHRO-211122/444
Improper Input Validation	01-Nov-2022	6.5	Insufficient data validation in Extensions in Google Chrome prior to 107.0.5304.62 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted Chrome Extension.	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html, https://crbug.com/1350111	A-GOO-CHRO-211122/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Low) **CVE ID : CVE-2022-3661**		
Improper Input Validation	01-Nov-2022	4.3	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 107.0.5304.62 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2022-3660**	https://crbug.com/1327505, https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html	A-GOO-CHRO-211122/446
Affected Version(s): * Up to (excluding) 107.0.5304.87					
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	8.8	Type confusion in V8 in Google Chrome prior to 107.0.5304.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3723**	https://crbug.com/1378239, https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_27.html	A-GOO-CHRO-211122/447
Vendor: gpac					
Product: gpac					
Affected Version(s): * Up to (excluding) 2022-11-07					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	11-Nov-2022	6.5	A vulnerability classified as problematic was found in GPAC. Affected by this vulnerability is the function svg_parse_preserveaspectratio of the file scenegraph/svg_attributes.c of the component SVG Parser. The manipulation leads to memory leak. The attack can be launched remotely. The name of the patch is 2191e66aa7df750e8ef01781b1930bea87b713bb. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-213463. **CVE ID : CVE-2022-3957**	https://github.com/gpac/gpac/commit/2191e66aa7df750e8ef01781b1930bea87b713bb	A-GPA-GPAC-211122/448
Affected Version(s): 2.1-dev-rev368-gfd054169b-master					
Missing Release of Memory after Effective Lifetime	02-Nov-2022	5.5	GPAC v2.1-DEV-rev368-gfd054169b-master was discovered to contain a memory leak via the component gf_list_new at utils/list.c.	https://github.com/gpac/gpac/issues/2284	A-GPA-GPAC-211122/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43254		
Missing Release of Memory after Effective Lifetime	02-Nov-2022	5.5	GPAC v2.1-DEV-rev368-gfd054169b-master was discovered to contain a memory leak via the component gf_odf_new_iod at odf/odf_code.c. **CVE ID : CVE-2022-43255**	https://github.com/gpac/gpac/issues/2285	A-GPA-GPAC-211122/450
Vendor: grafana					
Product: grafana					
Affected Version(s): * Up to (excluding) 8.5.15					
N/A	09-Nov-2022	5.3	Grafana is an open-source platform for monitoring and observability. When using the forget password on the login page, a POST request is made to the `/api/user/password/sent-reset-email` URL. When the username or email does not exist, a JSON response contains a “user not found” message. This leaks information to unauthenticated users and introduces a security risk. This issue has been patched in 9.2.4 and backported to	https://github.com/grafana/grafana/security/advisories/GHSA-3p62-42x7-gxg5	A-GRA-GRAF-211122/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.5.15. There are no known workarounds. **CVE ID : CVE-2022-39307**		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.5.15					
Improper Input Validation	09-Nov-2022	8.1	Grafana is an open-source platform for monitoring and observability. Versions prior to 9.2.4, or 8.5.15 on the 8.X branch, are subject to Improper Input Validation. Grafana admins can invite other members to the organization they are an admin for. When admins add members to the organization, non existing users get an email invite, existing members are added directly to the organization. When an invite link is sent, it allows users to sign up with whatever username/email address the user chooses and become a member of the organization. This introduces a vulnerability which can be used with malicious intent. This issue is patched in version	https://github.com/grafana/grafana/security/advisories/GHSA-2x6g-h2hg-rq84	A-GRA-GRAF-211122/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.2.4, and has been backported to 8.5.15. There are no known workarounds. **CVE ID : CVE-2022-39306**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.2.4					
Improper Input Validation	09-Nov-2022	8.1	Grafana is an open-source platform for monitoring and observability. Versions prior to 9.2.4, or 8.5.15 on the 8.X branch, are subject to Improper Input Validation. Grafana admins can invite other members to the organization they are an admin for. When admins add members to the organization, non existing users get an email invite, existing members are added directly to the organization. When an invite link is sent, it allows users to sign up with whatever username/email address the user chooses and become a member of the organization. This introduces a vulnerability which can be used with malicious intent.	https://github.com/grafana/grafana/security/advisories/GHSA-2x6g-h2hg-rq84	A-GRA-GRAF-211122/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is patched in version 9.2.4, and has been backported to 8.5.15. There are no known workarounds. **CVE ID : CVE-2022-39306**		
N/A	09-Nov-2022	5.3	Grafana is an open-source platform for monitoring and observability. When using the forget password on the login page, a POST request is made to the `/api/user/password/sent-reset-email` URL. When the username or email does not exist, a JSON response contains a “user not found” message. This leaks information to unauthenticated users and introduces a security risk. This issue has been patched in 9.2.4 and backported to 8.5.15. There are no known workarounds. **CVE ID : CVE-2022-39307**	https://github.com/grafana/grafana/security/advisories/GHSA-3p62-42x7-gxg5	A-GRA-GRAF-211122/454
Affected Version(s): From (including) 9.2.0 Up to (excluding) 9.2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Nov-2022	8.1	Grafana is an open-source platform for monitoring and observability. Versions starting with 9.2.0 and less than 9.2.4 contain a race condition in the authentication middlewares logic which may allow an unauthenticated user to query an administration endpoint under heavy load. This issue is patched in 9.2.4. There are no known workarounds. **CVE ID : CVE-2022-39328**	https://github.com/grafana/grafana/security/advisories/GHSA-vqc4-mpj8-jxch	A-GRA-GRAF-211122/455
Vendor: gvectors					
Product: wpforo_forum					
Affected Version(s): * Up to (including) 2.0.5					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	5.4	Cross-Site Request Forgery (CSRF) vulnerability in gVectors Team wpForo Forum plugin <= 2.0.5 on WordPress leading to topic deletion. **CVE ID : CVE-2022-40632**	https://wordpress.org/plugins/wpforo/, https://patchstack.com/database/vulnerability/wpforo/wordpress-wpforo-forum-plugin-2-0-5-cross-site-request-forgery-csrf-vulnerability-2?_s_id=cve	A-GVE-WPFO-211122/456
Authorization Bypass	08-Nov-2022	4.3	Insecure direct object references	https://patchstack.com/data	A-GVE-WPFO-211122/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Through User-Controlled Key			(IDOR) vulnerability in the wpForo Forum plugin <= 2.0.5 on WordPress allows attackers with subscriber or higher user roles to mark any forum post as solved/unsolved. **CVE ID : CVE-2022-40205**	base/vulnerability/wpforo/wordpress-wpforo-forum-plugin-2-0-5-insecure-direct-object-references-idor-vulnerability-2?_s_id=cve, https://wordpress.org/plugins/wpforo/	
Authorization Bypass Through User-Controlled Key	08-Nov-2022	4.3	Insecure direct object references (IDOR) vulnerability in the wpForo Forum plugin <= 2.0.5 on WordPress allows attackers with subscriber or higher user roles to mark any forum post as private/public. **CVE ID : CVE-2022-40206**	https://wordpress.org/plugins/wpforo/, https://patchstack.com/database/vulnerability/wpforo/wordpress-wpforo-forum-plugin-2-0-5-insecure-direct-object-references-idor-vulnerability?_s_id=cve	A-GVE-WPFO-211122/458
Vendor: hallowelt					
Product: bluespice					
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.2.1					
Improper Neutralization of Input During Web Page Generation	15-Nov-2022	6.1	Some UI elements of the Common User Interface Component are not properly sanitizing output and therefore prone to	https://en.wiki.bluespice.com/wiki/Security:Security_Advisories/BSSA-2022-08	A-HAL-BLUE-211122/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			output arbitrary HTML (XSS). **CVE ID : CVE-2022-3895**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Nov-2022	5.4	Cross-site Scripting (XSS) vulnerability in BlueSpiceUserSidebar extension of BlueSpice allows user with regular account and edit permissions to inject arbitrary HTML into the personal menu navigation of their own and other users. This allows for targeted attacks. **CVE ID : CVE-2022-3958**	https://en.wiki.bluespice.com/wiki/Security:Security_Advisories/BSSA-2022-07	A-HAL-BLUE-211122/460
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Nov-2022	5.4	Cross-site Scripting (XSS) vulnerability in BlueSpiceDiscovery skin of BlueSpice allows logged in user with edit permissions to inject arbitrary HTML into the default page header of a wikipage. **CVE ID : CVE-2022-41789**	https://en.wiki.bluespice.com/wiki/Security:Security_Advisories/BSSA-2022-04	A-HAL-BLUE-211122/461
Improper Neutralization of Input During Web Page	15-Nov-2022	5.4	Cross-site Scripting (XSS) vulnerability in BlueSpiceFoundation extension of BlueSpice allows	https://en.wiki.bluespice.com/wiki/Security:Security_Advisories/BSSA-2022-04	A-HAL-BLUE-211122/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user with regular account and edit permissions to inject arbitrary HTML into the history view of a wikipage. **CVE ID : CVE-2022-41814**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Nov-2022	5.4	Cross-site Scripting (XSS) vulnerability in BlueSpiceSocialProfile extension of BlueSpice allows user with comment permissions to inject arbitrary HTML into the comment section of a wikipage. **CVE ID : CVE-2022-42000**	https://en.wiki.bluespice.com/wiki/Security:Security_Advisories/BSSA-2022-04	A-HAL-BLUE-211122/463
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Nov-2022	5.4	Cross-site Scripting (XSS) vulnerability in BlueSpiceBookshelf extension of BlueSpice allows user with regular account and edit permissions to inject arbitrary HTML into the book navigation. **CVE ID : CVE-2022-42001**	https://en.wiki.bluespice.com/wiki/Security:Security_Advisories/BSSA-2022-05	A-HAL-BLUE-211122/464
Improper Neutralization of Input During	15-Nov-2022	4.8	Cross-site Scripting (XSS) vulnerability in BlueSpiceCustomMenu extension of	https://en.wiki.bluespice.com/wiki/Security:Security_A	A-HAL-BLUE-211122/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			BlueSpice allows user with admin permissions to inject arbitrary HTML into the custom menu navigation of the application. **CVE ID : CVE-2022-3893**	dvisories/BSSA-2022-06	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Nov-2022	4.8	Cross-site Scripting (XSS) vulnerability in BlueSpiceDiscovery skin of BlueSpice allows user with admin privileges to inject arbitrary HTML into the main navigation of the application. **CVE ID : CVE-2022-41611**	https://en.wiki.bluespice.com/wiki/Security:Security_Advisories/BSSA-2022-03	A-HAL-BLUE-211122/466
Product: common_user_interface					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Nov-2022	6.1	Some UI elements of the Common User Interface Component are not properly sanitizing output and therefore prone to output arbitrary HTML (XSS). **CVE ID : CVE-2022-3895**	https://en.wiki.bluespice.com/wiki/Security:Security_Advisories/BSSA-2022-08	A-HAL-COMM-211122/467
Vendor: hashicorp					
Product: nomad					
Affected Version(s): 1.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	10-Nov-2022	4.3	HashiCorp Nomad and Nomad Enterprise 1.4.0 up to 1.4.1 workload identity token can list non-sensitive metadata for paths under nomad/ that belong to other jobs in the same namespace. Fixed in 1.4.2. **CVE ID : CVE-2022-3866**	https://discuss.hashicorp.com/t/hcsec-2022-25-nomad-s-workload-identity-token-can-list-non-sensitive-metadata-for-nomad-paths/46167	A-HAS-NOMA-211122/468
Insufficient Session Expiration	10-Nov-2022	4.3	HashiCorp Nomad and Nomad Enterprise 1.4.0 up to 1.4.1 event stream subscribers using a token with TTL receive updates until token garbage is collected. Fixed in 1.4.2. **CVE ID : CVE-2022-3867**	https://discuss.hashicorp.com/t/hcsec-2022-26-nomad-s-event-stream-subscriber-using-acl-token-with-ttl-receive-updates-until-garbage-collected/46168	A-HAS-NOMA-211122/469
Affected Version(s): 1.4.1					
Exposure of Resource to Wrong Sphere	10-Nov-2022	4.3	HashiCorp Nomad and Nomad Enterprise 1.4.0 up to 1.4.1 workload identity token can list non-sensitive metadata for paths under nomad/ that belong to other jobs in the same namespace. Fixed in 1.4.2.	https://discuss.hashicorp.com/t/hcsec-2022-25-nomad-s-workload-identity-token-can-list-non-sensitive-metadata-for-nomad-paths/46167	A-HAS-NOMA-211122/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3866		
Insufficient Session Expiration	10-Nov-2022	4.3	HashiCorp Nomad and Nomad Enterprise 1.4.0 up to 1.4.1 event stream subscribers using a token with TTL receive updates until token garbage is collected. Fixed in 1.4.2. **CVE ID : CVE-2022-3867**	https://discuss.hashicorp.com/t/hcsec-2022-26-nomad-s-event-stream-subscriber-using-acl-token-with-ttl-receive-updates-until-garbage-collected/46168	A-HAS-NOMA-211122/471
Vendor: hcltech					
Product: domino					
Affected Version(s): * Up to (excluding) 9.0.1					
Cross-Site Request Forgery (CSRF)	04-Nov-2022	8.8	HCL XPages applications are susceptible to a Cross Site Request Forgery (CSRF) vulnerability. An unauthenticated attacker could exploit this vulnerability to perform actions in the application on behalf of the logged in user. **CVE ID : CVE-2022-38660**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0101037	A-HCL-DOMI-211122/472
Affected Version(s): 10.0.0					
N/A	04-Nov-2022	5.5	HCL Domino is susceptible to an information disclosure vulnerability. In	https://support.hcltechsw.com/csm?id=kb_article&sysp	A-HCL-DOMI-211122/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			some scenarios, local calls made on the server to search the Domino directory will ignore xACL read restrictions. An authenticated attacker could leverage this vulnerability to access attributes from a user's person record. **CVE ID : CVE-2022-38654**	arm_article=KB0101017	
Affected Version(s): 10.0.1					
N/A	04-Nov-2022	5.5	HCL Domino is susceptible to an information disclosure vulnerability. In some scenarios, local calls made on the server to search the Domino directory will ignore xACL read restrictions. An authenticated attacker could leverage this vulnerability to access attributes from a user's person record. **CVE ID : CVE-2022-38654**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0101017	A-HCL-DOMI-211122/474
Affected Version(s): 11.0.1					
N/A	04-Nov-2022	5.5	HCL Domino is susceptible to an information	https://support.hcltechsw.com/csm?id=k	A-HCL-DOMI-211122/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure vulnerability. In some scenarios, local calls made on the server to search the Domino directory will ignore xACL read restrictions. An authenticated attacker could leverage this vulnerability to access attributes from a user's person record. **CVE ID : CVE-2022-38654**	b_article&syspparm_article=KB0101017	
Affected Version(s): 12.0					
N/A	04-Nov-2022	5.5	HCL Domino is susceptible to an information disclosure vulnerability. In some scenarios, local calls made on the server to search the Domino directory will ignore xACL read restrictions. An authenticated attacker could leverage this vulnerability to access attributes from a user's person record. **CVE ID : CVE-2022-38654**	https://support.hcltechsw.com/csm?id=kb_article&syspparm_article=KB0101017	A-HCL-DOMI-211122/476
Affected Version(s): 9.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	04-Nov-2022	8.8	HCL XPages applications are susceptible to a Cross Site Request Forgery (CSRF) vulnerability. An unauthenticated attacker could exploit this vulnerability to perform actions in the application on behalf of the logged in user. **CVE ID : CVE-2022-38660**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0101037	A-HCL-DOMI-211122/477
N/A	04-Nov-2022	5.5	HCL Domino is susceptible to an information disclosure vulnerability. In some scenarios, local calls made on the server to search the Domino directory will ignore xACL read restrictions. An authenticated attacker could leverage this vulnerability to access attributes from a user's person record. **CVE ID : CVE-2022-38654**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0101017	A-HCL-DOMI-211122/478
Vendor: hhims_project					
Product: hhims					
Affected Version(s): 2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Nov-2022	9.8	A vulnerability classified as critical has been found in tsruban HHIMS 2.1. Affected is an unknown function of the component Patient Portrait Handler. The manipulation of the argument PID leads to sql injection. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. VDB-213462 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3956**	N/A	A-HHI-HHIM-211122/479
Vendor: highlight_focus_project					
Product: highlight_focus					
Affected Version(s): 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Nov-2022	4.8	The Highlight Focus WordPress plugin through 1.1 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	https://wpscan.com/vulnerability/b583de48-1332-4984-8c0c-a7ed4a2397cd	A-HIG-HIGH-211122/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example in multisite setup) **CVE ID : CVE-2022-3462**		
Vendor: Hitachi					
Product: infrastructure_analytics_advisor					
Affected Version(s): * Up to (excluding) 10.9.0-00					
N/A	01-Nov-2022	0	Insertion of Sensitive Information into Temporary File vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Analytics probe component), Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer probe component) allows local users to gain sensitive information. **CVE ID : CVE-2022-41553**	N/A	A-HIT-INFR-211122/481
Affected Version(s): From (including) 2.0.0-00 Up to (including) 4.4.0-00					
N/A	01-Nov-2022	0	Server-Side Request Forgery (SSRF) vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Data Center Analytics, Analytics probe components), Hitachi Ops Center Analyzer on Linux	N/A	A-HIT-INFR-211122/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Hitachi Ops Center Analyzer detail view, Hitachi Ops Center Analyzer probe components) allows Server Side Request Forgery. **CVE ID : CVE-2022-41552**		
Product: ops_center_analyzer					
Affected Version(s): From (including) 10.0.0-00 Up to (excluding) 10.9.0-00					
N/A	01-Nov-2022	0	Server-Side Request Forgery (SSRF) vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Data Center Analytics, Analytics probe components), Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer detail view, Hitachi Ops Center Analyzer probe components) allows Server Side Request Forgery. **CVE ID : CVE-2022-41552**	N/A	A-HIT-OPS_-211122/483
N/A	01-Nov-2022	0	Insertion of Sensitive Information into Temporary File vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Analytics	N/A	A-HIT-OPS_-211122/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			probe component), Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer probe component) allows local users to gain sensitive information. **CVE ID : CVE-2022-41553**		
Affected Version(s): From (including) 10.8.1-00 Up to (excluding) 10.9.0-00					
N/A	01-Nov-2022	0	Insertion of Sensitive Information into Log File vulnerability in Hitachi Ops Center Analyzer on Linux (Virtual Strage Software Agent component) allows local users to gain sensitive information. **CVE ID : CVE-2022-3191**	N/A	A-HIT-OPS_-211122/485
Product: ops_center_viewpoint					
Affected Version(s): From (including) 10.8.0-00 Up to (excluding) 10.9.0-00					
N/A	01-Nov-2022	0	Server-Side Request Forgery (SSRF) vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Data Center Analytics, Analytics probe components), Hitachi Ops Center Analyzer on Linux	N/A	A-HIT-OPS_-211122/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Hitachi Ops Center Analyzer detail view, Hitachi Ops Center Analyzer probe components) allows Server Side Request Forgery. **CVE ID : CVE-2022-41552**		
Vendor: html2xhtml_project					
Product: html2xhtml					
Affected Version(s): 1.3					
Out-of-bounds Read	08-Nov-2022	8.1	html2xhtml v1.3 was discovered to contain an Out-Of-Bounds read in the function static void elm_close(tree_node_t *nodo) at procesador.c. This vulnerability allows attackers to access sensitive files or cause a Denial of Service (DoS) via a crafted html file. **CVE ID : CVE-2022-44311**	N/A	A-HTM-HTML-211122/487
Vendor: huaxiaerp					
Product: huaxia_erp					
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	02-Nov-2022	6.5	A vulnerability was found in Huaxia ERP. It has been classified as problematic. This affects an unknown part of the file /depotHead/list of the component Retail Management.	N/A	A-HUA-HUAX-211122/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument search leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-212793 was assigned to this vulnerability. **CVE ID : CVE-2022-3826**		
Affected Version(s): 2.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Nov-2022	6.5	A vulnerability was found in Huaxia ERP 2.3 and classified as critical. Affected by this issue is some unknown functionality of the component User Management. The manipulation of the argument login 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-212792.	N/A	A-HUA-HUAX-211122/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3825		
Vendor: human_resource_management_system_project					
Product: human_resource_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Nov-2022	8.8	Human Resource Management System v1.0 was discovered to contain a SQL injection vulnerability via the stateedit parameter at /hrm/state.php. **CVE ID : CVE-2022-43318**	N/A	A-HUM-HUMA-211122/490
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Nov-2022	6.1	A cross-site scripting (XSS) vulnerability in /hrm/index.php?msg of Human Resource Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2022-43317**	N/A	A-HUM-HUMA-211122/491
Vendor: hypr					
Product: workforce_access					
Affected Version(s): * Up to (excluding) 7.7.1					
Incorrect Permission Assignment for Critical Resource	03-Nov-2022	8.8	Incorrect Permission Assignment for Critical Resource vulnerability in HYPR Workforce	https://www.hypr.com/security-advisories	A-HYP-WORK-211122/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Access on Windows allows Authentication Abuse. **CVE ID : CVE-2022-3258**		
Vendor: ibax					
Product: go-ibax					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	8.8	A vulnerability classified as critical has been found in IBAX go-ibax. Affected is an unknown function of the file /api/v2/open/tablesInfo. The manipulation 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-212634 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3798**	N/A	A-IBA-GO-I-211122/493
Improper Neutralization of Special Elements used in an SQL Command	01-Nov-2022	8.8	A vulnerability classified as critical was found in IBAX go-ibax. Affected by this vulnerability is an unknown functionality of the file /api/v2/open/tablesInfo. The	N/A	A-IBA-GO-I-211122/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			manipulation 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-212635. **CVE ID : CVE-2022-3799**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	8.8	A vulnerability, which was classified as critical, has been found in IBAX go-ibax. Affected by this issue is some unknown functionality of the file /api/v2/open/rowsInfo. The manipulation of the argument table_name 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-212636. **CVE ID : CVE-2022-3800**	N/A	A-IBA-GO-I-211122/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	8.8	A vulnerability, which was classified as critical, was found in IBAX go-ibax. This affects an unknown part of the file /api/v2/open/rowsInfo. The manipulation of the argument order 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-212637 was assigned to this vulnerability. **CVE ID : CVE-2022-3801**	N/A	A-IBA-GO-I-211122/496
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	8.8	A vulnerability has been found in IBAX go-ibax and classified as critical. This vulnerability affects unknown code of the file /api/v2/open/rowsInfo. The manipulation of the argument where leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may	N/A	A-IBA-GO-I-211122/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. VDB-212638 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3802**		
Vendor: ibexa					
Product: ezplatform-graphql					
Affected Version(s): 2.0.0					
Insecure Storage of Sensitive Information	10-Nov-2022	5.3	ezplatform-graphql is a GraphQL server implementation for Ibexa DXP and Ibexa Open Source. Versions prior to 2.3.12 and 1.0.13 are subject to Insecure Storage of Sensitive Information. Unauthenticated GraphQL queries for user accounts can expose password hashes of users that have created or modified content, typically administrators and editors. This issue has been patched in versions 2.3.12, and 1.0.13 on the 1.X branch. Users unable to upgrade can remove the "passwordHash" entry from "src/bundle/Resources/config/graphql/User.types.yaml"	https://github.com/ezsystems/ezplatform-graphql/security/advisories/GHSA-c7pc-pgf6-mfh5	A-IBE-EZPL-211122/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the GraphQL package, and other properties like hash type, email, login if you prefer. **CVE ID : CVE-2022-41876**		
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.0.13					
Insecure Storage of Sensitive Information	10-Nov-2022	5.3	ezplatform-graphql is a GraphQL server implementation for Ibexa DXP and Ibexa Open Source. Versions prior to 2.3.12 and 1.0.13 are subject to Insecure Storage of Sensitive Information. Unauthenticated GraphQL queries for user accounts can expose password hashes of users that have created or modified content, typically administrators and editors. This issue has been patched in versions 2.3.12, and 1.0.13 on the 1.X branch. Users unable to upgrade can remove the "passwordHash" entry from "src/bundle/Resources/config/graphql/User.types.yaml" in the GraphQL package, and other properties like hash	https://github.com/ezsystems/ezplatform-graphql/security/advisories/GHSA-c7pc-pgf6-mfh5	A-IBE-EZPL-211122/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			type, email, login if you prefer. **CVE ID : CVE-2022-41876**		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.3.12					
Insecure Storage of Sensitive Information	10-Nov-2022	5.3	ezplatform-graphql is a GraphQL server implementation for Ibexa DXP and Ibexa Open Source. Versions prior to 2.3.12 and 1.0.13 are subject to Insecure Storage of Sensitive Information. Unauthenticated GraphQL queries for user accounts can expose password hashes of users that have created or modified content, typically administrators and editors. This issue has been patched in versions 2.3.12, and 1.0.13 on the 1.X branch. Users unable to upgrade can remove the "passwordHash" entry from "src/bundle/Resources/config/graphql/User.types.yaml" in the GraphQL package, and other properties like hash type, email, login if you prefer.	https://github.com/ezsystems/ezplatform-graphql/security/advisories/GHSA-c7pc-pgf6-mfh5	A-IBE-EZPL-211122/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41876		
Vendor: IBM					
Product: business_automation_workflow					
Affected Version(s): 20.0.0.1					
Cleartext Storage of Sensitive Information	03-Nov-2022	4.3	"IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, and 22.0.1 could disclose sensitive version information to authenticated users which could be used in further attacks against the system. IBM X-Force ID: 230537." **CVE ID : CVE-2022-35279**	https://www.ibm.com/support/pages/node/6829847	A-IBM-BUSI-211122/501
Affected Version(s): 20.0.0.2					
Cleartext Storage of Sensitive Information	03-Nov-2022	4.3	"IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, and 22.0.1 could disclose sensitive version information to authenticated users which could be used in further attacks against the	https://www.ibm.com/support/pages/node/6829847	A-IBM-BUSI-211122/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. IBM X-Force ID: 230537." **CVE ID : CVE-2022-35279**		
Affected Version(s): 21.0.1					
Cleartext Storage of Sensitive Information	03-Nov-2022	4.3	"IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, and 22.0.1 could disclose sensitive version information to authenticated users which could be used in further attacks against the system. IBM X-Force ID: 230537." **CVE ID : CVE-2022-35279**	https://www.ibm.com/support/pages/node/6829847	A-IBM-BUSI-211122/503
Affected Version(s): 21.0.2					
Cleartext Storage of Sensitive Information	03-Nov-2022	4.3	"IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, and 22.0.1 could disclose sensitive version information to authenticated users which could be used in further attacks against the system. IBM X-Force ID: 230537."	https://www.ibm.com/support/pages/node/6829847	A-IBM-BUSI-211122/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35279		
Affected Version(s): 21.0.3					
Cleartext Storage of Sensitive Information	03-Nov-2022	4.3	"IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, and 22.0.1 could disclose sensitive version information to authenticated users which could be used in further attacks against the system. IBM X-Force ID: 230537." **CVE ID : CVE-2022-35279**	https://www.ibm.com/support/pages/node/6829847	A-IBM-BUSI-211122/505
Affected Version(s): 22.0.1					
Cleartext Storage of Sensitive Information	03-Nov-2022	4.3	"IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, and 22.0.1 could disclose sensitive version information to authenticated users which could be used in further attacks against the system. IBM X-Force ID: 230537." **CVE ID : CVE-2022-35279**	https://www.ibm.com/support/pages/node/6829847	A-IBM-BUSI-211122/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 18.0.0.0 Up to (including) 18.0.0.2					
Cleartext Storage of Sensitive Information	03-Nov-2022	4.3	"IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, and 22.0.1 could disclose sensitive version information to authenticated users which could be used in further attacks against the system. IBM X-Force ID: 230537." **CVE ID : CVE-2022-35279**	https://www.ibm.com/support/pages/node/6829847	A-IBM-BUSI-211122/507
Affected Version(s): From (including) 19.0.0.0 Up to (including) 19.0.0.3					
Cleartext Storage of Sensitive Information	03-Nov-2022	4.3	"IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, and 22.0.1 could disclose sensitive version information to authenticated users which could be used in further attacks against the system. IBM X-Force ID: 230537." **CVE ID : CVE-2022-35279**	https://www.ibm.com/support/pages/node/6829847	A-IBM-BUSI-211122/508
Product: cics_tx					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.1					
Use of a Broken or Risky Cryptographic Algorithm	14-Nov-2022	7.5	IBM CICS TX 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 229464. **CVE ID : CVE-2022-34320**	https://www.ibm.com/support/pages/node/6833206, https://exchange.xforce.ibmcloud.com/vulnerabilities/229464, https://www.ibm.com/support/pages/node/6833204	A-IBM-CICS-211122/509
N/A	14-Nov-2022	6.1	IBM CICS TX 11.1 Standard and Advanced could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a victim to a phishing site. IBM X-Force ID: 234172. **CVE ID : CVE-2022-38705**	https://www.ibm.com/support/pages/node/6833218, https://www.ibm.com/support/pages/node/6833216, https://exchange.xforce.ibmcloud.com/vulnerabilities/234172	A-IBM-CICS-211122/510
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	5.4	IBM CICS TX 11.1 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	https://www.ibm.com/support/pages/node/6833174, https://www.ibm.com/support/pages/node/6833172, https://exchange.xforce.ibmcloud.com/vul	A-IBM-CICS-211122/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure within a trusted session. IBM X-Force ID: 229451. **CVE ID : CVE-2022-34315**	nerabilities/229451	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	5.4	IBM CICS TX 11.1 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: 229459. **CVE ID : CVE-2022-34317**	https://exchange.xforce.ibmcloud.com/vulnerabilities/229459, https://www.ibm.com/support/pages/node/6833182, https://www.ibm.com/support/pages/node/6833180	A-IBM-CICS-211122/512
Improper Encoding or Escaping of Output	14-Nov-2022	5.3	IBM CICS TX 11.1 does not neutralize or incorrectly neutralizes web scripting syntax in HTTP headers that can be used by web browser components that can process raw headers. IBM X-Force ID: 229452. **CVE ID : CVE-2022-34316**	https://www.ibm.com/support/pages/node/6833178, https://www.ibm.com/support/pages/node/6833176	A-IBM-CICS-211122/513
Insecure Storage of Sensitive	14-Nov-2022	3.3	IBM CICS TX 11.1 allows web pages to be stored locally which can be read	https://www.ibm.com/support/pages/node/6833156,	A-IBM-CICS-211122/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			by another user on the system. IBM X-Force ID: 229447. **CVE ID : CVE-2022-34312**	https://exchange.xforce.ibmcloud.com/vulnerabilities/229447, https://www.ibm.com/support/pages/node/6833150	
Incorrect Permission Assignment for Critical Resource	14-Nov-2022	3.3	IBM CICS TX 11.1 could disclose sensitive information to a local user due to insecure permission settings. IBM X-Force ID: 229450. **CVE ID : CVE-2022-34314**	https://www.ibm.com/support/pages/node/6833166, https://www.ibm.com/support/pages/node/6833170	A-IBM-CICS-211122/515
N/A	14-Nov-2022	3.1	IBM CICS TX 11.1 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. X-Force ID: 229449.	https://www.ibm.com/support/pages/node/6833164, https://exchange.xforce.ibmcloud.com/vulnerabilities/229449, https://www.ibm.com/support/pages/node/6833158	A-IBM-CICS-211122/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34313		
Affected Version(s): 11.7					
Use of a Broken or Risky Cryptographic Algorithm	14-Nov-2022	7.5	IBM CICS TX 11.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 229463. **CVE ID : CVE-2022-34319**	https://www.ibm.com/support/pages/node/6833192, https://www.ibm.com/support/pages/node/6833190, https://exchange.xforce.ibmcloud.com/vulnerabilities/229463	A-IBM-CICS-211122/517
N/A	14-Nov-2022	5.3	IBM CICS TX 11.7 could allow an attacker to obtain sensitive information from HTTP response headers. IBM X-Force ID: 229467. **CVE ID : CVE-2022-34329**	https://www.ibm.com/support/pages/node/6833212, https://www.ibm.com/support/pages/node/6833210, https://exchange.xforce.ibmcloud.com/vulnerabilities/229467	A-IBM-CICS-211122/518
Product: cloud_pak_for_security					
Affected Version(s): From (including) 1.10.0.0 Up to (including) 1.10.2.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Nov-2022	8.8	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.2.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted	https://www.ibm.com/support/pages/node/6833584	A-IBM-CLOU-211122/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request. IBM X-Force ID: 233786. **CVE ID : CVE-2022-38387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	5.4	IBM Cloud Pak for Security (CP4S) 1.10.0.0 79and 1.10.2.0 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: 233663. **CVE ID : CVE-2022-36776**	https://exchange.xforce.ibmcloud.com/vulnerabilities/233663, https://www.ibm.com/support/pages/node/6833574	A-IBM-CLOU-211122/520
Product: cognos_analytics					
Affected Version(s): 11.1.7					
Cleartext Storage of Sensitive Information	03-Nov-2022	6.5	"IBM Cognos Analytics 11.2.1, 11.2.0, 11.1.7 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 229963." **CVE ID : CVE-2022-34339**	https://www.ibm.com/support/pages/node/6828527	A-IBM-COGN-211122/521
Affected Version(s): 11.2.0					
Cleartext Storage of	03-Nov-2022	6.5	"IBM Cognos Analytics 11.2.1,	https://www.ibm.com/supp	A-IBM-COGN-211122/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			11.2.0, 11.1.7 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 229963." **CVE ID : CVE-2022-34339**	ort/pages/node/6828527	
Affected Version(s): 11.2.1					
Cleartext Storage of Sensitive Information	03-Nov-2022	6.5	"IBM Cognos Analytics 11.2.1, 11.2.0, 11.1.7 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 229963." **CVE ID : CVE-2022-34339**	https://www.ibm.com/support/pages/node/6828527	A-IBM-COGN-211122/523
Affected Version(s): From (including) 11.1.0 Up to (excluding) 11.1.7					
Cleartext Storage of Sensitive Information	03-Nov-2022	6.5	"IBM Cognos Analytics 11.2.1, 11.2.0, 11.1.7 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 229963." **CVE ID : CVE-2022-34339**	https://www.ibm.com/support/pages/node/6828527	A-IBM-COGN-211122/524
Product: infosphere_information_server					
Affected Version(s): 11.7					
Improper Neutralization of Formula Elements	03-Nov-2022	9.8	"IBM InfoSphere Information Server 11.7 is potentially vulnerable to CSV Injection. A remote attacker could	https://www.ibm.com/support/pages/node/6829953	A-IBM-INFO-211122/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in a CSV File			execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 223598." **CVE ID : CVE-2022-22425**		
Improper Restriction of XML External Entity Reference	03-Nov-2022	9.1	"IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 236584." **CVE ID : CVE-2022-40747**	https://www.ibm.com/support/pages/node/6829373	A-IBM-INFO-211122/526
Cross-Site Request Forgery (CSRF)	03-Nov-2022	8.8	"IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a "user that the website trusts. IBM X-Force ID: 227295.	https://www.ibm.com/support/pages/node/6829335	A-IBM-INFO-211122/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30608		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Nov-2022	7.8	"IBM InfoSphere Information Server 11.7 could allow a locally authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-"Force ID: 231361. **CVE ID : CVE-2022-35717**	https://www.ibm.com/support/pages/node/6829365	A-IBM-INFO-211122/528
Exposure of Resource to Wrong Sphere	03-Nov-2022	6.5	"IBM InfoSphere Information Server 11.7 could allow an authenticated user to access information restricted to users with elevated privileges due to improper access controls. IBM X-Force ID: 224427." **CVE ID : CVE-2022-22442**	https://www.ibm.com/support/pages/node/6829325	A-IBM-INFO-211122/529
Improper Input Validation	03-Nov-2022	6.5	"IBM InfoSphere Information Server 11.7 could allow a user to cause a denial of service by removing the ability to run jobs due to improper input validation. IBM X-Force ID: 235725."	https://www.ibm.com/support/pages/node/6829369	A-IBM-INFO-211122/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40235		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	"IBM InfoSphere Information Server 11.7 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: 227592. **CVE ID : CVE-2022-30615**	https://www.ibm.com/support/pages/node/6829311	A-IBM-INFO-211122/531
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	"IBM InfoSphere Information Server 11.7 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: 227592." **CVE ID : CVE-2022-35642**	https://www.ibm.com/support/pages/node/6829311	A-IBM-INFO-211122/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: infosphere_information_server_on_cloud					
Affected Version(s): 11.7					
Exposure of Resource to Wrong Sphere	03-Nov-2022	6.5	"IBM InfoSphere Information Server 11.7 could allow an authenticated user to access information restricted to users with elevated privileges due to improper access controls. IBM X-Force ID: 224427." **CVE ID : CVE-2022-22442**	https://www.ibm.com/support/pages/node/6829325	A-IBM-INFO-211122/533
Product: mq					
Affected Version(s): 8.0.0.0					
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/support/pages/node/6833806	A-IBM-MQ-211122/534
Affected Version(s): 9.0.0.0					
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels.	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/support/pages/node/6833806	A-IBM-MQ-211122/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**		
Affected Version(s): 9.1.0					
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/support/pages/node/6833806	A-IBM-MQ-211122/536
Affected Version(s): 9.1.0.0					
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/support/pages/node/6833806	A-IBM-MQ-211122/537
Affected Version(s): 9.2.0					
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/supp	A-IBM-MQ-211122/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	ort/pages/node/6833806	
Product: mq_appliance					
Affected Version(s): 9.2.0.0					
Insufficient Session Expiration	03-Nov-2022	6.5	"IBM MQ Appliance 9.2 CD, 9.2 LTS, 9.3 CD, and LTS 9.3 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 235532." **CVE ID : CVE-2022-40230**	https://www.ibm.com/support/pages/node/6622051	A-IBM-MQ_A-211122/539
Affected Version(s): 9.3.0.0					
Insufficient Session Expiration	03-Nov-2022	6.5	"IBM MQ Appliance 9.2 CD, 9.2 LTS, 9.3 CD, and LTS 9.3 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 235532." **CVE ID : CVE-2022-40230**	https://www.ibm.com/support/pages/node/6622051	A-IBM-MQ_A-211122/540
Product: mq_internet_pass-thru					
Affected Version(s): 2.1					
Insertion of Sensitive	14-Nov-2022	5.5	IBM MQ Internet Pass-Thru 2.1, 9.2	https://www.ibm.com/supp	A-IBM-MQ_I-211122/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			LTS and 9.2 CD stores potentially sensitive information in trace files that could be read by a local user. **CVE ID : CVE-2022-35719**	ort/pages/node/6838559, https://exchange.xforce.ibmcloud.com/vulnerabilities/231370	
Affected Version(s): 9.2					
Insertion of Sensitive Information into Log File	14-Nov-2022	5.5	IBM MQ Internet Pass-Thru 2.1, 9.2 LTS and 9.2 CD stores potentially sensitive information in trace files that could be read by a local user. **CVE ID : CVE-2022-35719**	https://www.ibm.com/support/pages/node/6838559, https://exchange.xforce.ibmcloud.com/vulnerabilities/231370	A-IBM-MQ_I-211122/542
Product: robotic_process_automation					
Affected Version(s): * Up to (excluding) 21.0.3					
Cleartext Storage of Sensitive Information	03-Nov-2022	5.3	"IBM Robotic Process Automation 21.0.1 and 21.0.2 could disclose sensitive version information that could aid in further attacks against the system. IBM X-Force ID: 234292." **CVE ID : CVE-2022-38710**	https://www.ibm.com/support/pages/node/6831681	A-IBM-ROBO-211122/543
Affected Version(s): * Up to (excluding) 21.0.6					
Incorrect Default	03-Nov-2022	7.5	"IBM Robotic Process Automation 21.0.1, 21.0.2, 21.0.3,	https://www.ibm.com/supp	A-IBM-ROBO-211122/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			21.0.4, and 21.0.5 is vulnerable to incorrect permission assignment which could allow access to application configurations. IBM X-Force ID: 238679." **CVE ID : CVE-2022-43574**	ort/pages/node/6831645	
Product: robotic_process_automation_as_a_service					
Affected Version(s): * Up to (excluding) 21.0.3					
Cleartext Storage of Sensitive Information	03-Nov-2022	5.3	"IBM Robotic Process Automation 21.0.1 and 21.0.2 could disclose sensitive version information that could aid in further attacks against the system. IBM X-Force ID: 234292." **CVE ID : CVE-2022-38710**	https://www.ibm.com/support/pages/node/6831681	A-IBM-ROBO-211122/545
Product: robotic_process_automation_for_cloud_pak					
Affected Version(s): * Up to (excluding) 21.0.3					
Cleartext Storage of Sensitive Information	03-Nov-2022	5.3	"IBM Robotic Process Automation 21.0.1 and 21.0.2 could disclose sensitive version information that could aid in further attacks against the system. IBM X-Force ID: 234292."	https://www.ibm.com/support/pages/node/6831681	A-IBM-ROBO-211122/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38710		
Affected Version(s): * Up to (excluding) 21.0.6					
Incorrect Default Permissions	03-Nov-2022	7.5	"IBM Robotic Process Automation 21.0.1, 21.0.2, 21.0.3, 21.0.4, and 21.0.5 is vulnerable to incorrect permission assignment which could allow access to application configurations. IBM X-Force ID: 238679." **CVE ID : CVE-2022-43574**	https://www.ibm.com/support/pages/node/6831645	A-IBM-ROBO-211122/547
Exposure of Resource to Wrong Sphere	03-Nov-2022	3.3	"IBM Robotic Process Automation for Cloud Pak 21.0.1, 21.0.2, 21.0.3, 21.0.4, and 21.0.5 is vulnerable to exposure of the first tenant owner e-mail address to users with access to the container platform. IBM X-Force ID: 238214." **CVE ID : CVE-2022-42442**	https://www.ibm.com/support/pages/node/6831787	A-IBM-ROBO-211122/548
Product: websphere_application_server					
Affected Version(s): 8.5					
Improper Neutralization of Input	11-Nov-2022	5.4	IBM WebSphere Application Server 8.5, and 9.0 is vulnerable to cross-	https://exchange.xforce.ibmcloud.com/vulnerabilities/2	A-IBM-WEBS-211122/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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: 236588. **CVE ID : CVE-2022-40750**	36588, https://www.ibm.com/support/pages/node/6833552	
Affected Version(s): 9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	5.4	IBM WebSphere Application Server 8.5, and 9.0 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: 236588. **CVE ID : CVE-2022-40750**	https://exchange.xforce.ibmcloud.com/vulnerabilities/236588, https://www.ibm.com/support/pages/node/6833552	A-IBM-WEBS-211122/550
Affected Version(s): From (including) 7.0.0.0 Up to (excluding) 7.0.0.45					
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could	https://www.ibm.com/support/pages/node/6829907	A-IBM-WEBS-211122/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**		
Affected Version(s): From (including) 8.0.0.0 Up to (excluding) 8.0.0.15					
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**	https://www.ibm.com/support/pages/node/6829907	A-IBM-WEBS-211122/552
Affected Version(s): From (including) 8.5.0.0 Up to (excluding) 8.5.5.23					
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762."	https://www.ibm.com/support/pages/node/6829907	A-IBM-WEBS-211122/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38712		
Affected Version(s): From (including) 9.0.0.0 Up to (excluding) 9.0.5.14					
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**	https://www.ibm.com/support/pages/node/6829907	A-IBM-WEBS-211122/554
Vendor: infotel					
Product: tasklists					
Affected Version(s): * Up to (excluding) 2.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	6.1	tasklists is a tasklists plugin for GLPI (Kanban). Versions prior to 2.0.3 are vulnerable to Cross-site Scripting. Cross-site Scripting (XSS) - Create XSS in task content (when add it). This issue is patched in version 2.0.3. There are no known workarounds. **CVE ID : CVE-2022-39398**	https://github.com/InfotelGLPI/tasklists/security/advisories/GHSA-3qv3-8393-777q, https://github.com/InfotelGLPI/tasklists/commit/4a1b30f3d9fa764695f98ce011c8542772530d47	A-INF-TASK-211122/555
Vendor: Intel					
Product: quartus_prime					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 22.1					
XML Injection (aka Blind XPath Injection)	11-Nov-2022	7.5	XML injection in the Intel(R) Quartus Prime Pro and Standard edition software may allow an unauthenticated user to potentially enable information disclosure via network access. **CVE ID : CVE-2022-27233**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00659.html	A-INT-QUAR-211122/556
Affected Version(s): * Up to (including) 21.1					
Uncontrolled Search Path Element	11-Nov-2022	7.8	Uncontrolled search path element in the Intel(R) Quartus Prime Standard edition software before version 21.1 Patch 0.02std may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-27187**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00659.html	A-INT-QUAR-211122/557
XML Injection (aka Blind XPath Injection)	11-Nov-2022	7.5	XML injection in the Intel(R) Quartus Prime Pro and Standard edition software may allow an unauthenticated user to potentially enable information disclosure via network access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00659.html	A-INT-QUAR-211122/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27233		
Product: wlan_authentication_and_privacy_infrastructure					
Affected Version(s): * Up to (excluding) 22.2150.0.1					
N/A	11-Nov-2022	3.3	Improper access control in the Intel(R) WAPI Security software for Windows 10/11 before version 22.2150.0.1 may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2022-33973**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00720.html	A-INT-WLAN-211122/559
Vendor: Intelliants					
Product: subrion_cms					
Affected Version(s): 4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-2022	6.1	A cross-site scripting (XSS) vulnerability in the /panel/fields/add component of Intelliants Subrion CMS v4.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Field default value text field. **CVE ID : CVE-2022-43120**	N/A	A-INT-SUBR-211122/560
Improper Neutralization of	09-Nov-2022	6.1	A cross-site scripting (XSS) vulnerability in the	N/A	A-INT-SUBR-211122/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			CMS Field Add page of Intelliants Subrion CMS v4.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the tooltip text field. **CVE ID : CVE-2022-43121**		
Vendor: Invisible-island					
Product: xterm					
Affected Version(s): * Up to (excluding) 375					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Nov-2022	9.8	xterm before 375 allows code execution via font ops, e.g., because an OSC 50 response may have Ctrl-g and therefore lead to command execution within the vi line-editing mode of Zsh. NOTE: font ops are not allowed in the xterm default configurations of some Linux distributions. **CVE ID : CVE-2022-45063**	https://invisible-island.net/xterm/xterm.log.html, https://www.openwall.com/lists/oss-security/2022/11/10/1, http://www.openwall.com/lists/oss-security/2022/11/10/1, http://www.openwall.com/lists/oss-security/2022/11/10/5	A-INV-XTER-211122/562
Vendor: ironmansoftware					
Product: powershell_universal					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.12.6					
Improper Privilege	14-Nov-2022	8.8	Escalation of privileges in the Web Server in	https://docs.powershelluniversal.com/cha	A-IRO-POWE-211122/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Ironman Software PowerShell Universal 2.x and 3.x allows an attacker with a valid app token to retrieve other app tokens by ID via an HTTP web request. Patched Versions are 3.5.3, 3.4.7, and 2.12.6. **CVE ID : CVE-2022-45183**	ngelog, https://blog.ironmansoftware.com/psu-2022-11-cve/, https://ironmansoftware.com	
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.4.7					
Improper Privilege Management	14-Nov-2022	8.8	Escalation of privileges in the Web Server in Ironman Software PowerShell Universal 2.x and 3.x allows an attacker with a valid app token to retrieve other app tokens by ID via an HTTP web request. Patched Versions are 3.5.3, 3.4.7, and 2.12.6. **CVE ID : CVE-2022-45183**	https://docs.powershelluniversal.com/changelog, https://blog.ironmansoftware.com/psu-2022-11-cve/, https://ironmansoftware.com	A-IRO-POWE-211122/564
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Nov-2022	7.2	The Web Server in Ironman Software PowerShell Universal v3.x and v2.x allows for directory traversal outside of the configuration directory, which allows a remote	https://docs.powershelluniversal.com/changelog, https://blog.ironmansoftware.com/psu-2022-11-cve/, https://ironm	A-IRO-POWE-211122/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrator privilege to create, delete, update, and display files outside of the configuration directory via a crafted HTTP request to particular endpoints in the web server. Patched Versions are 3.5.3 and 3.4.7. **CVE ID : CVE-2022-45184**	ansoftware.com	
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.3					
Improper Privilege Management	14-Nov-2022	8.8	Escalation of privileges in the Web Server in Ironman Software PowerShell Universal 2.x and 3.x allows an attacker with a valid app token to retrieve other app tokens by ID via an HTTP web request. Patched Versions are 3.5.3, 3.4.7, and 2.12.6. **CVE ID : CVE-2022-45183**	https://docs.powershelluniversal.com/changelog, https://blog.ironmansoftware.com/psu-2022-11-cve/, https://ironmansoftware.com	A-IRO-POWE-211122/566
Improper Limitation of a Pathname to a Restricted Directory	14-Nov-2022	7.2	The Web Server in Ironman Software PowerShell Universal v3.x and v2.x allows for directory traversal outside of the configuration	https://docs.powershelluniversal.com/changelog, https://blog.ironmansoftware.com/psu-2022-11-cve/,	A-IRO-POWE-211122/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			directory, which allows a remote attacker with administrator privilege to create, delete, update, and display files outside of the configuration directory via a crafted HTTP request to particular endpoints in the web server. Patched Versions are 3.5.3 and 3.4.7. **CVE ID : CVE-2022-45184**	https://ironmansoftware.com	
Vendor: istio					
Product: istio					
Affected Version(s): From (including) 1.15.0 Up to (including) 1.15.2					
Incorrect Authorization	10-Nov-2022	3.5	Istio is an open platform to connect, manage, and secure microservices. In versions on the 1.15.x branch prior to 1.15.3, a user can impersonate any workload identity within the service mesh if they have localhost access to the Istiod control plane. Version 1.15.3 contains a patch for this issue. There are no known workarounds.	https://github.com/istio/istio/security/advisories/GHSA-6c6p-h79f-g6p4, https://github.com/istio/istio/commit/9a643e270421560afb2630e00f76d46a55499df9, https://istio.io/latest/news/releases/1.15.x/announcing-1.15.3/	A-IST-ISTI-211122/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39388		
Vendor: Jetbrains					
Product: teamcity					
Affected Version(s): * Up to (excluding) 2022.10					
N/A	03-Nov-2022	7.5	In JetBrains TeamCity version before 2022.10, Project Viewer could see scrambled secure values in the MetaRunner settings **CVE ID : CVE-2022-44623**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-211122/569
Insertion of Sensitive Information into Log File	03-Nov-2022	7.5	In JetBrains TeamCity version before 2022.10, Password parameters could be exposed in the build log if they contained special characters **CVE ID : CVE-2022-44624**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-211122/570
N/A	03-Nov-2022	5.3	In JetBrains TeamCity version before 2022.10, no audit items were added upon editing a user's settings **CVE ID : CVE-2022-44646**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-211122/571
Affected Version(s): From (including) 2021.2 Up to (excluding) 2022.10					
N/A	03-Nov-2022	5.3	In JetBrains TeamCity version between 2021.2 and 2022.10 access	https://www.jetbrains.com/privacy-	A-JET-TEAM-211122/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions for secure token health items were excessive **CVE ID : CVE-2022-44622**	security/issues-fixed/	
Vendor: Joomla					
Product: joomla\!					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	An issue was discovered in Joomla! 4.0.0 through 4.2.4. Inadequate filtering of potentially malicious user input leads to reflected XSS vulnerabilities in com_media. **CVE ID : CVE-2022-27914**	https://developer.joomla.org/security-centre/887-20221101-core-rxss-through-reflection-of-user-input-in-com-media.html	A-JOO-JOOM-211122/573
Vendor: jumpdemand					
Product: 4ecps_web_forms					
Affected Version(s): * Up to (including) 0.2.17					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in JumpDEMAND Inc. 4ECPS Web Forms plugin <= 0.2.17 on WordPress. **CVE ID : CVE-2022-44628**	https://wordpress.org/plugins/4ecps-webforms/, https://patchstack.com/database/vulnerability/4ecps-webforms/wordpress-4ecps-web-forms-plugin-0-2-17-auth-stored-cross-site-scripting-xss-	A-JUM-4ECP-211122/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				vulnerability?_s_id=cve	
Vendor: kavitareader					
Product: kavita					
Affected Version(s): * Up to (excluding) 0.6.0.3					
Improper Restriction of Excessive Authentication Attempts	11-Nov-2022	5.3	Improper Restriction of Excessive Authentication Attempts in GitHub repository kareadita/kavita prior to 0.6.0.3. **CVE ID : CVE-2022-3945**	https://huntr.dev/bounties/55cd91b3-1d94-4d34-8d7f-86660b41fd65, https://github.com/kareadita/kavita/commit/f8db37d3f9aa42d47e7c4f4ca839e892d3f97afb	A-KAV-KAVI-211122/575
Vendor: keystonejs					
Product: keystone					
Affected Version(s): 3.0.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Nov-2022	9.8	Keystone is a headless CMS for Node.js — built with GraphQL and React.`@keystone-6/core@3.0.0 || 3.0.1` users that use `NODE_ENV` to trigger security-sensitive functionality in their production builds are vulnerable to `NODE_ENV` being inlined to `"development"` for user code, irrespective of what	https://github.com/keystonejs/keystone/pull/8063, https://github.com/keystonejs/keystone/security/advisories/GHSA-25mx-2mxm-6343, https://github.com/keystonejs/keystone/pull/8031/	A-KEY-KEYS-211122/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			your environment variables. If you do not use `NODE_ENV` in your user code to trigger security-sensitive functionality, you are not impacted by this vulnerability. Any dependencies that use `NODE_ENV` to trigger particular behaviors (optimizations, security or otherwise) should still respect your environment's configured `NODE_ENV` variable. The application's dependencies, as found in `node_modules` (including `@keystone-6/core`), are typically not compiled as part of this process, and thus should be unaffected. We have tested this assumption by verifying that `NODE_ENV=production yarn keystone start` still uses secure cookies when using `statelessSessions`.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability has been fixed in @keystone-6/core@3.0.2, regression tests have been added for this vulnerability in #8063. **CVE ID : CVE-2022-39382**		
Affected Version(s): 3.0.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Nov-2022	9.8	Keystone is a headless CMS for Node.js — built with GraphQL and React.`@keystone-6/core@3.0.0 || 3.0.1` users that use `NODE_ENV` to trigger security-sensitive functionality in their production builds are vulnerable to `NODE_ENV` being inlined to `"development"` for user code, irrespective of what your environment variables. If you do not use `NODE_ENV` in your user code to trigger security-sensitive functionality, you are not impacted by this vulnerability. Any dependencies that use	https://github.com/keystonejs/keystone/pull/8063, https://github.com/keystonejs/keystone/security/advisories/GHSA-25mx-2mxm-6343, https://github.com/keystonejs/keystone/pull/8031/	A-KEY-KEYS-211122/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`NODE_ENV` to trigger particular behaviors (optimizations, security or otherwise) should still respect your environment's configured `NODE_ENV` variable. The application's dependencies, as found in `node_modules` (including `@keystone-6/core`), are typically not compiled as part of this process, and thus should be unaffected. We have tested this assumption by verifying that `NODE_ENV=production yarn keystone start` still uses secure cookies when using `statelessSessions`. This vulnerability has been fixed in @keystone-6/core@3.0.2, regression tests have been added for this vulnerability in #8063. **CVE ID : CVE-2022-39382**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: keywordrush					
Product: content_egg					
Affected Version(s): * Up to (including) 5.4.0					
Cross-Site Request Forgery (CSRF)	03-Nov-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Keywordrush Content Egg plugin <= 5.4.0 on WordPress. **CVE ID : CVE-2022-25952**	https://patchstack.com/database/vulnerability/content-egg/wordpress-content-egg-plugin-5-4-0-cross-site-request-forgery-csrf-vulnerability?_s_id=cve, https://wordpress.org/plugins/content-egg/#developers	A-KEY-CONT-211122/578
Vendor: konker					
Product: konker_platform					
Affected Version(s): 2.3.9					
Cross-Site Request Forgery (CSRF)	15-Nov-2022	8.8	Konker v2.3.9 was to discovered to contain a Cross-Site Request Forgery (CSRF). **CVE ID : CVE-2022-35613**	N/A	A-KON-KONK-211122/579
Vendor: lesspipe_project					
Product: lesspipe					
Affected Version(s): * Up to (excluding) 2.06					
Deserialization of Untrusted Data	01-Nov-2022	9.8	lesspipe before 2.06 allows attackers to execute code via Perl Storable (pst) files, because of deserialized object	https://bugs.gentoo.org/865631	A-LES-LESS-211122/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			destructor execution via a key/value pair in a hash. **CVE ID : CVE-2022-44542**		
Vendor: lightning_network_daemon_project					
Product: lightning_network_daemon					
Affected Version(s): * Up to (excluding) 0.15.2					
N/A	07-Nov-2022	9.8	btcd before 0.23.2, as used in Lightning Labs lnd before 0.15.2-beta and other Bitcoin-related products, mishandles witness size checking. **CVE ID : CVE-2022-44797**	https://github.com/btcsuite/btcd/pull/1896	A-LIG-LIGH-211122/581
Vendor: Limesurvey					
Product: limesurvey					
Affected Version(s): 5.4.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Nov-2022	7.2	LimeSurvey v5.4.4 was discovered to contain a SQL injection vulnerability via the component /application/views/themeOptions/update.php. **CVE ID : CVE-2022-43279**	N/A	A-LIM-LIME-211122/582
Vendor: lineagrafica					
Product: eu_cookie_law_gdpr					
Affected Version(s): * Up to (excluding) 2.1.3					
Improper Neutralization of	10-Nov-2022	9.1	The EU Cookie Law GDPR (Banner + Blocker) module	https://www.lineagrafica.es/modp/lgcook	A-LIN-EU_C-211122/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			before 2.1.3 for PrestaShop allows SQL Injection via a cookie (lgcookieslaw or __lglaw). **CVE ID : CVE-2022-44727**	ieslaw/en/readme_en.pdf	
Vendor: Mahara					
Product: mahara					
Affected Version(s): 22.10.0					
N/A	06-Nov-2022	9.8	Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0 potentially allow a PDF export to trigger a remote shell if the site is running on Ubuntu and the flag -dSAFER is not set with Ghostscript. **CVE ID : CVE-2022-44544**	https://bugs.launchpad.net/mahara/+bug/1979575, https://mahara.org/interaction/forum/topic.php?id=9198	A-MAH-MAHA-211122/584
N/A	06-Nov-2022	7.5	In Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0, embedded images are accessible without a sufficient permission check under certain conditions.	https://bugs.launchpad.net/mahara/+bug/1991157, https://mahara.org/interaction/forum/topic.php?id=9199	A-MAH-MAHA-211122/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42707		
Affected Version(s): From (including) 21.04.0 Up to (excluding) 21.04.7					
N/A	06-Nov-2022	9.8	Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0 potentially allow a PDF export to trigger a remote shell if the site is running on Ubuntu and the flag -dSAFER is not set with Ghostscript. **CVE ID : CVE-2022-44544**	https://bugs.launchpad.net/mahara/+bug/1979575, https://mahara.org/interaction/forum/topic.php?id=9198	A-MAH-MAHA-211122/586
N/A	06-Nov-2022	7.5	In Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0, embedded images are accessible without a sufficient permission check under certain conditions. **CVE ID : CVE-2022-42707**	https://bugs.launchpad.net/mahara/+bug/1991157, https://mahara.org/interaction/forum/topic.php?id=9199	A-MAH-MAHA-211122/587
Affected Version(s): From (including) 21.10.0 Up to (excluding) 21.10.5					
N/A	06-Nov-2022	9.8	Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0 potentially	https://bugs.launchpad.net/mahara/+bug/1979575, https://mahara.org/interaction/forum/top	A-MAH-MAHA-211122/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a PDF export to trigger a remote shell if the site is running on Ubuntu and the flag - dSAFER is not set with Ghostscript. **CVE ID : CVE-2022-44544**	ic.php?id=9198	
N/A	06-Nov-2022	7.5	In Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0, embedded images are accessible without a sufficient permission check under certain conditions. **CVE ID : CVE-2022-42707**	https://bugs.launchpad.net/mahara/+bug/1991157, https://mahara.org/interaction/forum/topic.php?id=9199	A-MAH-MAHA-211122/589
Affected Version(s): From (including) 22.04.0 Up to (excluding) 22.04.3					
N/A	06-Nov-2022	9.8	Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0 potentially allow a PDF export to trigger a remote shell if the site is running on Ubuntu and the flag - dSAFER is not set with Ghostscript. **CVE ID : CVE-2022-44544**	https://bugs.launchpad.net/mahara/+bug/1979575, https://mahara.org/interaction/forum/topic.php?id=9198	A-MAH-MAHA-211122/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Nov-2022	7.5	In Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0, embedded images are accessible without a sufficient permission check under certain conditions. **CVE ID : CVE-2022-42707**	https://bugs.launchpad.net/mahara/+bug/1991157, https://mahara.org/interaction/forum/topic.php?id=9199	A-MAH-MAHA-211122/591
Vendor: manydesigns					
Product: portofino					
Affected Version(s): 5.3.2					
Exposure of Resource to Wrong Sphere	11-Nov-2022	7.1	A vulnerability has been found in ManyDesigns Portofino 5.3.2 and classified as problematic. Affected by this vulnerability is the function createTempDir of the file WarFileLauncher.java. The manipulation leads to creation of temporary file in directory with insecure permissions. Upgrading to version 5.3.3 is able to address this issue. The name of the patch is	https://github.com/ManyDesigns/Portofino/pull/580, https://github.com/ManyDesigns/Portofino/commit/94653cb357806c9cf24d8d294e6afea33f8f0775	A-MAN-PORT-211122/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			94653cb357806c9cf24d8d294e6afea33f8f0775. It is recommended to upgrade the affected component. The identifier VDB-213457 was assigned to this vulnerability. **CVE ID : CVE-2022-3952**		
Vendor: markdownify_project					
Product: markdownify					
Affected Version(s): 1.4.1					
Files or Directories Accessible to External Parties	03-Nov-2022	5.5	Markdownify version 1.4.1 allows an external attacker to remotely obtain arbitrary local files on any client that attempts to view a malicious markdown file through Markdownify. This is possible because the application does not have a CSP policy (or at least not strict enough) and/or does not properly validate the contents of markdown files before rendering them. **CVE ID : CVE-2022-41710**	N/A	A-MAR-MARK-211122/593
Vendor: maxonerp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: maxon					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Nov-2022	9.8	A vulnerability classified as critical has been found in Maxon ERP. This affects an unknown part of the file /index.php/purchase_order/browse_data. The manipulation of the argument tb_search 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 associated identifier of this vulnerability is VDB-213039. **CVE ID : CVE-2022-3878**	N/A	A-MAX-MAXO-211122/594
Vendor: Mcafee					
Product: data_exchange_layer					
Affected Version(s): * Up to (excluding) 6.0.0.280					
Incorrect Authorization	07-Nov-2022	5.5	Privilege escalation vulnerability in DXL Broker for Windows prior to 6.0.0.280 allows local users to gain elevated privileges by exploiting weak directory controls in the logs directory. This can lead to a denial-of-	https://kcm.trellix.com/corporate/index?page=content&id=SB10383	A-MCA-DATA-211122/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service attack on the DXL Broker. **CVE ID : CVE-2022-2188**		
Vendor: mendix					
Product: saml					
Affected Version(s): * Up to (excluding) 1.17.0					
Authentication Bypass by Capture-replay	08-Nov-2022	9.8	A vulnerability has been identified in Mendix SAML Module (Mendix 7 compatible) (All versions < V1.17.0), Mendix SAML Module (Mendix 7 compatible) (All versions >= V1.17.0), Mendix SAML Module (Mendix 8 compatible) (All versions < V2.3.0), Mendix SAML Module (Mendix 8 compatible) (All versions >= V2.3.0 < V2.3.2), Mendix SAML Module (Mendix 9 compatible, New Track) (All versions < V3.3.1), Mendix SAML Module (Mendix 9 compatible, New Track) (All versions >= V3.3.1 < V3.3.5), Mendix SAML Module (Mendix 9 compatible, Upgrade Track) (All versions < V3.3.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-638652.pdf	A-MEN-SAML-211122/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mendix SAML Module (Mendix 9 compatible, Upgrade Track) (All versions >= V3.3.0 < V3.3.4). Affected versions of the module insufficiently protect from packet capture replay, only when the not recommended, non default configuration option `'Allow Idp Initiated Authentication'` is enabled. This CVE entry describes the incomplete fix for CVE-2022-37011 in a specific non default configuration. **CVE ID : CVE-2022-44457**		
Affected Version(s): From (including) 2.3.0 Up to (excluding) 2.3.2					
Authentication Bypass by Capture-replay	08-Nov-2022	9.8	A vulnerability has been identified in Mendix SAML Module (Mendix 7 compatible) (All versions < V1.17.0), Mendix SAML Module (Mendix 7 compatible) (All versions >= V1.17.0), Mendix SAML Module (Mendix 8 compatible) (All versions < V2.3.0),	https://cert-portal.siemens.com/productcert/pdf/ssa-638652.pdf	A-MEN-SAML-211122/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mendix SAML Module (Mendix 8 compatible) (All versions >= V2.3.0 < V2.3.2), Mendix SAML Module (Mendix 9 compatible, New Track) (All versions < V3.3.1), Mendix SAML Module (Mendix 9 compatible, New Track) (All versions >= V3.3.1 < V3.3.5), Mendix SAML Module (Mendix 9 compatible, Upgrade Track) (All versions < V3.3.0), Mendix SAML Module (Mendix 9 compatible, Upgrade Track) (All versions >= V3.3.0 < V3.3.4). Affected versions of the module insufficiently protect from packet capture replay, only when the not recommended, non default configuration option `'Allow Idp Initiated Authentication'` is enabled. This CVE entry describes the incomplete fix for CVE-2022-37011 in a specific non		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default configuration. **CVE ID : CVE-2022-44457**		
Affected Version(s): From (including) 3.3.0 Up to (excluding) 3.3.4					
Authentication Bypass by Capture-replay	08-Nov-2022	9.8	A vulnerability has been identified in Mendix SAML Module (Mendix 7 compatible) (All versions < V1.17.0), Mendix SAML Module (Mendix 7 compatible) (All versions >= V1.17.0), Mendix SAML Module (Mendix 8 compatible) (All versions < V2.3.0), Mendix SAML Module (Mendix 8 compatible) (All versions >= V2.3.0 < V2.3.2), Mendix SAML Module (Mendix 9 compatible, New Track) (All versions < V3.3.1), Mendix SAML Module (Mendix 9 compatible, New Track) (All versions >= V3.3.1 < V3.3.5), Mendix SAML Module (Mendix 9 compatible, Upgrade Track) (All versions < V3.3.0), Mendix SAML Module (Mendix 9 compatible,	https://cert-portal.siemens.com/productcert/pdf/ssa-638652.pdf	A-MEN-SAML-211122/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Upgrade Track) (All versions >= V3.3.0 < V3.3.4). Affected versions of the module insufficiently protect from packet capture replay, only when the not recommended, non default configuration option `'Allow Idp Initiated Authentication'` is enabled. This CVE entry describes the incomplete fix for CVE-2022-37011 in a specific non default configuration. **CVE ID : CVE-2022-44457**		
Vendor: messagepack_project					
Product: messagepack					
Affected Version(s): * Up to (excluding) 2.1.1					
N/A	10-Nov-2022	7.5	Unmarshal can panic on some inputs, possibly allowing for denial of service attacks. **CVE ID : CVE-2022-41719**	https://github.com/shamaton/msgpack/issues/31, https://github.com/shamaton/msgpack/pull/32	A-MES-MESS-211122/599
Vendor: metagauss					
Product: profilegrid					
Affected Version(s): * Up to (excluding) 5.1.1					
Improper Neutralization of	14-Nov-2022	6.1	The ProfileGrid WordPress plugin before 5.1.1 does	https://wpscan.com/vulnerability/17596	A-MET-PROF-211122/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-3578**	b0e-ff45-4d0c-8e57-a31101e30345	
Vendor: Microsoft					
Product: 365_apps					
Affected Version(s): -					
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-365_-211122/601
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41106. **CVE ID : CVE-2022-41063**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41063	A-MIC-365_-211122/602
N/A	09-Nov-2022	7.8	Microsoft Excel Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41104**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41104	A-MIC-365_-211122/603
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	A-MIC-365_-211122/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41063. **CVE ID : CVE-2022-41106**	sory/CVE-2022-41106	
N/A	09-Nov-2022	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41107**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41107	A-MIC-365_-211122/605
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-365_-211122/606
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-365_-211122/607
N/A	09-Nov-2022	5.5	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-41105**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41105	A-MIC-365_-211122/608
Product: azure_cyclecloud					
Affected Version(s): 7.0					
N/A	09-Nov-2022	8.8	Azure CycleCloud Elevation of	https://portal.msrc.microsoft.com/en-	A-MIC-AZUR-211122/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-41085**	US/security-guidance/advisory/CVE-2022-41085	
Affected Version(s): 8.0					
N/A	09-Nov-2022	8.8	Azure CycleCloud Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41085**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41085	A-MIC-AZUR-211122/610
Product: azure_iot_edge_for_linux					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7	Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38014**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38014	A-MIC-AZUR-211122/611
Product: azure_rtos_guix_studio					
Affected Version(s): -					
N/A	09-Nov-2022	7.8	Azure RTOS GUIX Studio Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41051**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41051	A-MIC-AZUR-211122/612
Product: azure_rtos_usbx					
Affected Version(s): * Up to (excluding) 6.1.12					
Buffer Copy without Checking	04-Nov-2022	9.8	Azure RTOS USBX is a USB host, device, and on-the-go (OTG)	https://github.com/azure-rtos/usbx/security/advisori	A-MIC-AZUR-211122/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			embedded stack, that is fully integrated with Azure RTOS ThreadX. Prior to version 6.1.12, the USB DFU UPLOAD functionality may be utilized to introduce a buffer overflow resulting in overwrite of memory contents. In particular cases this may allow an attacker to bypass security features or execute arbitrary code. The implementation of `ux_device_class_dfu_control_request` function prevents buffer overflow during handling of DFU UPLOAD command when current state is `UX_SYSTEM_DFU_STATE_DFU_IDLE`. This issue has been patched, please upgrade to version 6.1.12. As a workaround, add the `UPLOAD_LENGTH` check in all possible states. **CVE ID : CVE-2022-39344**	es/GHSA-m9p8-xrp7-vvqp	
Product: dynamics_365_business_central					
Affected Version(s): 2019					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	4.4	Microsoft Business Central Information Disclosure Vulnerability. **CVE ID : CVE-2022-41066**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41066	A-MIC-DYNA-211122/614
Affected Version(s): 2022					
N/A	09-Nov-2022	4.4	Microsoft Business Central Information Disclosure Vulnerability. **CVE ID : CVE-2022-41066**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41066	A-MIC-DYNA-211122/615
Product: dynamics_nav					
Affected Version(s): 2018					
N/A	09-Nov-2022	4.4	Microsoft Business Central Information Disclosure Vulnerability. **CVE ID : CVE-2022-41066**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41066	A-MIC-DYNA-211122/616
Product: excel					
Affected Version(s): 2013					
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41106. **CVE ID : CVE-2022-41063**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41063	A-MIC-EXCE-211122/617
N/A	09-Nov-2022	7.8	Microsoft Excel Security Feature Bypass Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	A-MIC-EXCE-211122/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41104	sory/CVE-2022-41104	
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41063. **CVE ID : CVE-2022-41106**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41106	A-MIC-EXCE-211122/619
Affected Version(s): 2016					
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41106. **CVE ID : CVE-2022-41063**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41063	A-MIC-EXCE-211122/620
N/A	09-Nov-2022	7.8	Microsoft Excel Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41104**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41104	A-MIC-EXCE-211122/621
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41063. **CVE ID : CVE-2022-41106**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41106	A-MIC-EXCE-211122/622
Product: exchange_server					
Affected Version(s): 2019					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	9.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41123. **CVE ID : CVE-2022-41080**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41080	A-MIC-EXCH-211122/623
N/A	09-Nov-2022	7.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41080. **CVE ID : CVE-2022-41123**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41123	A-MIC-EXCH-211122/624
N/A	09-Nov-2022	7.5	Microsoft Exchange Server Spoofing Vulnerability. This CVE ID is unique from CVE-2022-41079. **CVE ID : CVE-2022-41078**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41078	A-MIC-EXCH-211122/625
N/A	09-Nov-2022	7.5	Microsoft Exchange Server Spoofing Vulnerability. This CVE ID is unique from CVE-2022-41078. **CVE ID : CVE-2022-41079**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41079	A-MIC-EXCH-211122/626
Affected Version(s): 2013					
N/A	09-Nov-2022	9.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	A-MIC-EXCH-211122/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41123. **CVE ID : CVE-2022-41080**	sory/CVE-2022-41080	
N/A	09-Nov-2022	7.5	Microsoft Exchange Server Spoofing Vulnerability. This CVE ID is unique from CVE-2022-41079. **CVE ID : CVE-2022-41078**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41078	A-MIC-EXCH-211122/628
N/A	09-Nov-2022	7.5	Microsoft Exchange Server Spoofing Vulnerability. This CVE ID is unique from CVE-2022-41078. **CVE ID : CVE-2022-41079**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41079	A-MIC-EXCH-211122/629
Affected Version(s): 2016					
N/A	09-Nov-2022	9.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41123. **CVE ID : CVE-2022-41080**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41080	A-MIC-EXCH-211122/630
N/A	09-Nov-2022	7.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41080. **CVE ID : CVE-2022-41123**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41123	A-MIC-EXCH-211122/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.5	Microsoft Exchange Server Spoofing Vulnerability. This CVE ID is unique from CVE-2022-41079. **CVE ID : CVE-2022-41078**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41078	A-MIC-EXCH-211122/632
N/A	09-Nov-2022	7.5	Microsoft Exchange Server Spoofing Vulnerability. This CVE ID is unique from CVE-2022-41078. **CVE ID : CVE-2022-41079**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41079	A-MIC-EXCH-211122/633
Product: office					
Affected Version(s): 2019					
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-OFFI-211122/634
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41106. **CVE ID : CVE-2022-41063**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41063	A-MIC-OFFI-211122/635
N/A	09-Nov-2022	7.8	Microsoft Excel Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41104**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41104	A-MIC-OFFI-211122/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41063. **CVE ID : CVE-2022-41106**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41106	A-MIC-OFFI-211122/637
N/A	09-Nov-2022	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41107**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41107	A-MIC-OFFI-211122/638
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-OFFI-211122/639
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-OFFI-211122/640
N/A	09-Nov-2022	5.5	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-41105**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41105	A-MIC-OFFI-211122/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2021					
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-OFFI-211122/642
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41106. **CVE ID : CVE-2022-41063**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41063	A-MIC-OFFI-211122/643
N/A	09-Nov-2022	7.8	Microsoft Excel Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41104**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41104	A-MIC-OFFI-211122/644
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41063. **CVE ID : CVE-2022-41106**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41106	A-MIC-OFFI-211122/645
N/A	09-Nov-2022	7.8	Microsoft Office Graphics Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41107**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41107	A-MIC-OFFI-211122/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-OFFI-211122/647
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-OFFI-211122/648
N/A	09-Nov-2022	5.5	Microsoft Excel Information Disclosure Vulnerability. **CVE ID : CVE-2022-41105**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41105	A-MIC-OFFI-211122/649
Product: office_online_server					
Affected Version(s): -					
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-OFFI-211122/650
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41106.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41063	A-MIC-OFFI-211122/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41063		
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41063. **CVE ID : CVE-2022-41106**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41106	A-MIC-OFFI-211122/652
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-OFFI-211122/653
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-OFFI-211122/654
Product: office_web_apps_server					
Affected Version(s): 2013					
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-OFFI-211122/655
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution	https://portal.msrc.microsoft.com/en-	A-MIC-OFFI-211122/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-41106. **CVE ID : CVE-2022-41063**	US/security-guidance/advisory/CVE-2022-41063	
N/A	09-Nov-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41063. **CVE ID : CVE-2022-41106**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41106	A-MIC-OFFI-211122/657
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-OFFI-211122/658
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-OFFI-211122/659
Product: sharepoint_enterprise_server					
Affected Version(s): 2013					
N/A	09-Nov-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	A-MIC-SHAR-211122/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41062	sory/CVE-2022-41062	
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-SHAR-211122/661
N/A	09-Nov-2022	6.5	Microsoft SharePoint Server Spoofing Vulnerability. **CVE ID : CVE-2022-41122**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41122	A-MIC-SHAR-211122/662
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-SHAR-211122/663
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-SHAR-211122/664
Affected Version(s): 2016					
N/A	09-Nov-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	A-MIC-SHAR-211122/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41062	sory/CVE-2022-41062	
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-SHAR-211122/666
N/A	09-Nov-2022	6.5	Microsoft SharePoint Server Spoofing Vulnerability. **CVE ID : CVE-2022-41122**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41122	A-MIC-SHAR-211122/667
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-SHAR-211122/668
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-SHAR-211122/669
Product: sharepoint_foundation					
Affected Version(s): 2013					
N/A	09-Nov-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	A-MIC-SHAR-211122/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41062	sory/CVE-2022-41062	
N/A	09-Nov-2022	6.5	Microsoft SharePoint Server Spoofing Vulnerability. **CVE ID : CVE-2022-41122**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41122	A-MIC-SHAR-211122/671
Product: sharepoint_server					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41062**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41062	A-MIC-SHAR-211122/672
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-SHAR-211122/673
N/A	09-Nov-2022	6.5	Microsoft SharePoint Server Spoofing Vulnerability. **CVE ID : CVE-2022-41122**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41122	A-MIC-SHAR-211122/674
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-SHAR-211122/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-SHAR-211122/676
Affected Version(s): 2019					
N/A	09-Nov-2022	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41062**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41062	A-MIC-SHAR-211122/677
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-SHAR-211122/678
N/A	09-Nov-2022	6.5	Microsoft SharePoint Server Spoofing Vulnerability. **CVE ID : CVE-2022-41122**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41122	A-MIC-SHAR-211122/679
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-SHAR-211122/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-SHAR-211122/681
Product: visual_studio_2017					
Affected Version(s): From (including) 15.0 Up to (including) 15.9					
N/A	09-Nov-2022	7.8	Visual Studio Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41119**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41119	A-MIC-VISU-211122/682
Product: visual_studio_2019					
Affected Version(s): From (including) 16.0 Up to (including) 16.11					
N/A	09-Nov-2022	7.8	Visual Studio Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41119**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41119	A-MIC-VISU-211122/683
Product: visual_studio_2022					
Affected Version(s): 17.0					
N/A	09-Nov-2022	7.8	Visual Studio Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41119**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41119	A-MIC-VISU-211122/684
Affected Version(s): 17.2					
N/A	09-Nov-2022	7.8	Visual Studio Remote Code	https://portal.msrc.microsoft.com/en-	A-MIC-VISU-211122/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability. **CVE ID : CVE-2022-41119**	US/security-guidance/advisory/CVE-2022-41119	
Affected Version(s): 17.3					
N/A	09-Nov-2022	7.8	Visual Studio Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41119**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41119	A-MIC-VISU-211122/686
Product: windows_subsystem_for_linux					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7	Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38014**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38014	A-MIC-WIND-211122/687
Product: windows_sysmon					
Affected Version(s): -					
N/A	09-Nov-2022	7.8	Microsoft Windows Sysmon Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41120**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41120	A-MIC-WIND-211122/688
Product: word					
Affected Version(s): 2013					
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-WORD-211122/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability. **CVE ID : CVE-2022-41061**	guidance/advisory/CVE-2022-41061	
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-WORD-211122/690
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-WORD-211122/691
Affected Version(s): 2016					
N/A	09-Nov-2022	7.8	Microsoft Word Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41061**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	A-MIC-WORD-211122/692
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41103. **CVE ID : CVE-2022-41060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41060	A-MIC-WORD-211122/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	Microsoft Word Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-41060. **CVE ID : CVE-2022-41103**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41103	A-MIC-WORD-211122/694
Vendor: muhammarajs_project					
Product: muhammarajs					
Affected Version(s): * Up to (including) 2.6.0					
NULL Pointer Dereference	02-Nov-2022	5.5	Muhammara is a node module with c/cpp bindings to modify PDF with js for node or electron (based/replacement on/of galkhana/hummusjs). The package muhammara before 2.6.0; all versions of package hummus are vulnerable to Denial of Service (DoS) when supplied with a maliciously crafted PDF file to be appended to another. This issue has been patched in 2.6.0 for muhammara and not at all for hummus. As a workaround, do not process files from untrusted sources. **CVE ID : CVE-2022-39381**	https://github.com/julianhille/MuhammaraJS/security/advisories/GHSA-rcrx-fpjp-mfrw, https://github.com/julianhille/MuhammaraJS/pull/194	A-MUH-MUHA-211122/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: muhammara_project					
Product: muhammara					
Affected Version(s): * Up to (excluding) 2.6.0					
N/A	01-Nov-2022	7.5	The package muhammara before 2.6.0; all versions of package hummus are vulnerable to Denial of Service (DoS) when PDFStreamForResponse() is used with invalid data. **CVE ID : CVE-2022-25885**	https://github.com/galkahana/HummusJS/issues/439, https://security.snyk.io/vuln/SNYK-JS-MUHAMMARA-3091137, https://security.snyk.io/vuln/SNYK-JS-HUMMUS-3091139, https://github.com/julianhille/MuhammaraJS/commit/0a6427eec82ef2978995e453de2dc0d6224dd46c	A-MUH-MUHA-211122/696
Affected Version(s): 3.1.0					
N/A	01-Nov-2022	7.5	The package muhammara before 2.6.1, from 3.0.0 and before 3.1.1; all versions of package hummus are vulnerable to Denial of Service (DoS) when supplied with a maliciously crafted PDF file to be parsed. **CVE ID : CVE-2022-25892**	https://github.com/julianhille/MuhammaraJS/commit/90b278d09f16062d93a4160ef0a54d449d739c51, https://security.snyk.io/vuln/SNYK-JS-MUHAMMARA-3060320, https://security.snyk.io/vuln/SNYK-JS-	A-MUH-MUHA-211122/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				HUMMUS-3091138, https://github.com/galkahana/HummusJS/issues/463	
Affected Version(s): * Up to (excluding) 2.6.1					
N/A	01-Nov-2022	7.5	The package muhammara before 2.6.1, from 3.0.0 and before 3.1.1; all versions of package hummus are vulnerable to Denial of Service (DoS) when supplied with a maliciously crafted PDF file to be parsed. **CVE ID : CVE-2022-25892**	https://github.com/julianhille/MuhammaraJS/commit/90b278d09f16062d93a4160ef0a54d449d739c51, https://security.snyk.io/vuln/SNYK-JS-MUHAMMARA-3060320, https://security.snyk.io/vuln/SNYK-JS-HUMMUS-3091138, https://github.com/galkahana/HummusJS/issues/463	A-MUH-MUHA-211122/698
Vendor: n-prolog_project					
Product: n-prolog					
Affected Version(s): 1.91					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Nov-2022	7.5	N-Prolog v1.91 was discovered to contain a global buffer overflow vulnerability in the function gettoken() at Main.c. **CVE ID : CVE-2022-43343**	N/A	A-N-P-N-PR-211122/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ndk-design					
Product: ndkadvancedcustomizationfields					
Affected Version(s): 3.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.5	A SQL injection vulnerability in the height and width parameter in NdkAdvancedCustomizationFields v3.5.0 allows unauthenticated attackers to exfiltrate database data. **CVE ID : CVE-2022-40839**	N/A	A-NDK-NDKA-211122/700
Affected Version(s): * Up to (including) 3.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	6.1	ndk design NdkAdvancedCustomizationFields 3.5.0 is vulnerable to Cross Site Scripting (XSS) via createPdf.php. **CVE ID : CVE-2022-40840**	N/A	A-NDK-NDKA-211122/701
Vendor: NEC					
Product: expresscluster_x					
Affected Version(s): * Up to (including) 5.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	9.8	Path traversal vulnerability in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and	https://jpn.nec.com/security-info/secinfo/nv22-014_en.html	A-NEC-EXPR-221122/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code. **CVE ID : CVE-2022-34822**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Nov-2022	9.8	Buffer overflow vulnerability in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code. **CVE ID : CVE-2022-34823**	https://jpn.nec.com/security-info/secinfo/nv22-014_en.html	A-NEC-EXPR-221122/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-Nov-2022	9.8	Weak File and Folder Permissions vulnerability in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code. **CVE ID : CVE-2022-34824**	https://jpn.nec.com/security-info/secinfo/nv22-014_en.html	A-NEC-EXPR-221122/704
Uncontrolled Search Path Element	08-Nov-2022	9.8	Uncontrolled Search Path Element in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0	https://jpn.nec.com/security-info/secinfo/nv22-014_en.html	A-NEC-EXPR-221122/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code. **CVE ID : CVE-2022-34825**		
Product: expresscluster_x_singleserversafe					
Affected Version(s): * Up to (including) 5.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	9.8	Path traversal vulnerability in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code. **CVE ID : CVE-2022-34822**	https://jpn.nec.com/security-info/secinfo/nv22-014_en.html	A-NEC-EXPR-221122/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Nov-2022	9.8	Buffer overflow vulnerability in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code. **CVE ID : CVE-2022-34823**	https://jpn.nec.com/security-info/secinfo/nv22-014_en.html	A-NEC-EXPR-221122/707
Incorrect Default Permissions	08-Nov-2022	9.8	Weak File and Folder Permissions vulnerability in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe	https://jpn.nec.com/security-info/secinfo/nv22-014_en.html	A-NEC-EXPR-221122/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code. **CVE ID : CVE-2022-34824**		
Uncontrolled Search Path Element	08-Nov-2022	9.8	Uncontrolled Search Path Element in CLUSTERPRO X 5.0 for Windows and earlier, EXPRESSCLUSTER X 5.0 for Windows and earlier, CLUSTERPRO X 5.0 SingleServerSafe for Windows and earlier, EXPRESSCLUSTER X 5.0 SingleServerSafe for Windows and earlier allows a remote unauthenticated attacker to overwrite existing files on the file system and to potentially execute arbitrary code. **CVE ID : CVE-2022-34825**	https://jpn.nec.com/security-info/secinfo/nv22-014_en.html	A-NEC-EXPR-221122/709
Vendor: Net-snmp					
Product: net-snmp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 5.4.3 Up to (including) 5.9.3					
NULL Pointer Dereference	07-Nov-2022	6.5	handle_ipv6IpForwarding in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.4.3 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service. **CVE ID : CVE-2022-44793**	N/A	A-NET-NET--221122/710
Affected Version(s): From (including) 5.8 Up to (including) 5.9.3					
NULL Pointer Dereference	07-Nov-2022	6.5	handle_ipDefaultTTL in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.8 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker (who has write access) to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service. **CVE ID : CVE-2022-44792**	N/A	A-NET-NET--221122/711
Vendor: Netapp					
Product: clustered_data_ontap					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	7.5	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any	https://www.openssl.org/news/secadv/20221101.txt, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0023, https://security.netapp.com/advisory/ntap-20221102-0001/	A-NET-CLUS-221122/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6). **CVE ID : CVE-2022-3602**		
Vendor: netwrix					
Product: auditor					
Affected Version(s): * Up to (excluding) 10.5					
Deserialization of Untrusted Data	08-Nov-2022	9.8	Remote code execution vulnerabilities exist in the Netwrix	N/A	A-NET-AUDI-221122/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Auditor User Activity Video Recording component affecting both the Netwrix Auditor server and agents installed on monitored systems. The remote code execution vulnerabilities exist within the underlying protocol used by the component, and potentially allow an unauthenticated remote attacker to execute arbitrary code as the NT AUTHORITY\SYSTEM user on affected systems, including on systems Netwrix Auditor monitors. **CVE ID : CVE-2022-31199**		
Vendor: newsmag_project					
Product: newsmag					
Affected Version(s): * Up to (excluding) 5.2.2					
Improper Authentication	14-Nov-2022	9.8	The tagDiv Composer WordPress plugin before 3.5, required by the Newspaper WordPress theme before 12.1 and Newsmag WordPress theme before 5.2.2, does not properly	https://wpscan.com/vulnerability/993a95d2-6fce-48de-ae17-06ce2db829ef	A-NEW-NEWS-221122/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implement the Facebook login feature, allowing unauthenticated attackers to login as any user by just knowing their email address **CVE ID : CVE-2022-3477**		
Vendor: newspaper_project					
Product: newspaper					
Affected Version(s): * Up to (excluding) 12.1					
Improper Authentication	14-Nov-2022	9.8	The tagDiv Composer WordPress plugin before 3.5, required by the Newspaper WordPress theme before 12.1 and Newsmag WordPress theme before 5.2.2, does not properly implement the Facebook login feature, allowing unauthenticated attackers to login as any user by just knowing their email address **CVE ID : CVE-2022-3477**	https://wpscan.com/vulnerability/993a95d2-6fce-48de-ae17-06ce2db829ef	A-NEW-NEWS-221122/715
Vendor: Nextcloud					
Product: desktop					
Affected Version(s): 3.6.0					
Improper Control of Generation of Code	11-Nov-2022	7.8	The Nextcloud Desktop Client is a tool to synchronize files from	https://github.com/nextcloud/server/pull/34559,	A-NEX-DESK-221122/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Nextcloud Server with your computer. In version 3.6.0, if a user received a malicious file share and has it synced locally or the virtual filesystem enabled and clicked a nc://open/ link it will open the default editor for the file type of the shared file, which on Windows can also sometimes mean that a file depending on the type, e.g. "vbs", is being executed. It is recommended that the Nextcloud Desktop client is upgraded to version 3.6.1. As a workaround, users can block the Nextcloud Desktop client 3.6.0 by setting the `minimum.supported.desktop.version` system config to `3.6.1` on the server, so new files designed to use this attack vector are not downloaded anymore. Already existing files can still be used. Another workaround would	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3w86-rm38-8w63, https://github.com/nextcloud/desktop/pull/5039	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be to enforce shares to be accepted by setting the `sharing.force_share_accept` system config to `true` on the server, so new files designed to use this attack vector are not downloaded anymore. Already existing shares can still be abused. **CVE ID : CVE-2022-41882**		
Vendor: Nvidia					
Product: cloud_gaming					
Affected Version(s): * Up to (excluding) 515.65.01					
NULL Pointer Dereference	10-Nov-2022	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2022-34666**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-CLOU-221122/717
Affected Version(s): * Up to (excluding) 516.94					
NULL Pointer Dereference	10-Nov-2022	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-CLOU-221122/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2022-34666**		
Product: virtual_gpu					
Affected Version(s): * Up to (excluding) 11.9					
NULL Pointer Dereference	10-Nov-2022	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2022-34666**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-221122/719
Affected Version(s): From (including) 13.0 Up to (excluding) 13.4					
NULL Pointer Dereference	10-Nov-2022	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-221122/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34666		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.2					
NULL Pointer Dereference	10-Nov-2022	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2022-34666**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-221122/721
Vendor: objectfirst					
Product: object_first					
Affected Version(s): * Up to (excluding) 1.0.13.1611					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	07-Nov-2022	9.8	An issue was discovered in Object First 1.0.7.712. The authorization service has a flow that allows getting access to the Web UI without knowing credentials. For signing, the JWT token uses a secret key that is generated through a function that doesn't produce cryptographically strong sequences. An attacker can predict these sequences and	https://objectfirst.com/security/of-20221024-0002/	A-OBJ-OBJE-221122/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generate a JWT token. As a result, an attacker can get access to the Web UI. This is fixed in 1.0.13.1611. **CVE ID : CVE-2022-44796**		
N/A	07-Nov-2022	8.8	An issue was discovered in Object First 1.0.7.712. Management protocol has a flow which allows a remote attacker to execute arbitrary Bash code with root privileges. The command that sets the hostname doesn't validate input parameters. As a result, arbitrary data goes directly to the Bash interpreter. An attacker would need credentials to exploit this vulnerability. This is fixed in 1.0.13.1611. **CVE ID : CVE-2022-44794**	https://objectfirst.com/security/of-20221024-0001/	A-OBJ-OBJE-221122/723
Use of Insufficiently Random Values	07-Nov-2022	6.5	An issue was discovered in Object First 1.0.7.712. A flaw was found in the Web Service, which could lead to local information	https://objectfirst.com/security/of-20221024-0003/	A-OBJ-OBJE-221122/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure. The command that creates the URL for the support bundle uses an insecure RNG. That can lead to prediction of the generated URL. As a result, an attacker can get access to system logs. An attacker would need credentials to exploit this vulnerability. This is fixed in 1.0.13.1611. **CVE ID : CVE-2022-44795**		
Vendor: octopus					
Product: octopus_server					
Affected Version(s): From (including) 2022.2.6729 Up to (excluding) 2022.2.8277					
N/A	01-Nov-2022	0	In affected versions of Octopus Server where access is managed by an external authentication provider, it was possible that the API key/keys of a disabled/deleted user were still valid after the access was revoked. **CVE ID : CVE-2022-2572**	N/A	A-OCT-OCTO-221122/725
Affected Version(s): From (including) 2022.3.348 Up to (excluding) 2022.3.10586					
N/A	01-Nov-2022	0	In affected versions of Octopus Server where access is	N/A	A-OCT-OCTO-221122/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			managed by an external authentication provider, it was possible that the API key/keys of a disabled/deleted user were still valid after the access was revoked. **CVE ID : CVE-2022-2572**		
Affected Version(s): From (including) 2022.4.791 Up to (excluding) 2022.4.2898					
N/A	01-Nov-2022	0	In affected versions of Octopus Server where access is managed by an external authentication provider, it was possible that the API key/keys of a disabled/deleted user were still valid after the access was revoked. **CVE ID : CVE-2022-2572**	N/A	A-OCT-OCTO-221122/727
Affected Version(s): From (including) 3.5 Up to (excluding) 2022.1.3264					
N/A	01-Nov-2022	0	In affected versions of Octopus Server where access is managed by an external authentication provider, it was possible that the API key/keys of a disabled/deleted user were still valid after the access was revoked.	N/A	A-OCT-OCTO-221122/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2572		
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')	09-Nov-2022	9.8	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms//classes/Master.php?f=delete_activity. **CVE ID : CVE-2022-43058**	N/A	A-ONL-ONLI-221122/729
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Nov-2022	8.8	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/?page=appointments/view_appointment. **CVE ID : CVE-2022-43226**	N/A	A-ONL-ONLI-221122/730
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/classes/Us	N/A	A-ONL-ONLI-221122/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ers.php?f=delete_test. **CVE ID : CVE-2022-43051**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/classes/Users.php?f=delete. **CVE ID : CVE-2022-43052**	N/A	A-ONL-ONLI-221122/732
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_appointment. **CVE ID : CVE-2022-43062**	N/A	A-ONL-ONLI-221122/733
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Users.php?f=delete_client. **CVE ID : CVE-2022-43063**	N/A	A-ONL-ONLI-221122/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/classes/Master.php?f=delete_message. **CVE ID : CVE-2022-43066**	N/A	A-ONL-ONLI-221122/735
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_reservation. **CVE ID : CVE-2022-43068**	N/A	A-ONL-ONLI-221122/736
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=user/manage_user. **CVE ID : CVE-2022-43124**	N/A	A-ONL-ONLI-221122/737
Improper Neutralization of Special	01-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to	N/A	A-ONL-ONLI-221122/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			contain a SQL injection vulnerability via the id parameter at /appointments/manage_appointment.php. **CVE ID : CVE-2022-43125**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/tests/manage_test.php. **CVE ID : CVE-2022-43126**	N/A	A-ONL-ONLI-221122/739
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /appointments/update_status.php. **CVE ID : CVE-2022-43127**	N/A	A-ONL-ONLI-221122/740
Improper Neutralization of Special Elements used in an SQL Command	02-Nov-2022	7.2	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms/admin/?pa	N/A	A-ONL-ONLI-221122/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			ge=appointments/view_appointment. **CVE ID : CVE-2022-43227**		
Vendor: online_tours_and_travels_management_system_project					
Product: online_tours_and_travels_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	07-Nov-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain an arbitrary file upload vulnerability in the component update_profile.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-43050**	N/A	A-ONL-ONLI-221122/742
Vendor: online_tours_\&_travels_management_system_project					
Product: online_tours_\&_travels_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	03-Nov-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain an arbitrary file upload vulnerability in the component /operations/travellers.php. This vulnerability allows	N/A	A-ONL-ONLI-221122/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-43061**		
Vendor: open5gs					
Product: open5gs					
Affected Version(s): 2.4.11					
Missing Release of Memory after Effective Lifetime	01-Nov-2022	7.5	open5gs v2.4.11 was discovered to contain a memory leak in the component src/upf/pfcp-path.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted PFCP packet. **CVE ID : CVE-2022-43221**	N/A	A-OPE-OPEN-221122/744
Missing Release of Memory after Effective Lifetime	01-Nov-2022	7.5	open5gs v2.4.11 was discovered to contain a memory leak in the component src/smf/pfcp-path.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted PFCP packet. **CVE ID : CVE-2022-43222**	N/A	A-OPE-OPEN-221122/745
Missing Release of Memory after	01-Nov-2022	7.5	open5gs v2.4.11 was discovered to contain a memory leak in the component ngap-	N/A	A-OPE-OPEN-221122/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			handler.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted UE attachment. **CVE ID : CVE-2022-43223**		
Vendor: openfga					
Product: openfga					
Affected Version(s): * Up to (excluding) 0.2.5					
Incorrect Authorization	08-Nov-2022	9.8	OpenFGA is a high-performance authorization/permission engine inspired by Google Zanzibar. Versions prior to 0.2.5 are vulnerable to authorization bypass under certain conditions. You are affected by this vulnerability if you added a tuple with a wildcard (*) assigned to a tupleset relation (the right hand side of a â€˜fromâ€™ statement). This issue has been patched in version v0.2.5. This update is not backward compatible with any authorization model that uses wildcard on a tupleset relation. **CVE ID : CVE-2022-39352**	https://github.com/openfga/openfga/security/advisories/GHSA-3gfj-fxx4-f22w	A-OPE-OPEN-221122/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: openharmony					
Product: openharmony					
Affected Version(s): From (including) 3.1 Up to (including) 3.1.2					
NULL Pointer Dereference	03-Nov-2022	7.5	OpenHarmony-v3.1.2 and prior versions had a DOS vulnerability in distributedhardware_device_manager when joining a network. Network attakcers can send an abonormal packet when joining a network, cause a nullptr reference and device reboot. **CVE ID : CVE-2022-43495**	N/A	A-OPE-OPEN-221122/748
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Nov-2022	6.5	OpenHarmony-v3.1.2 and prior versions had an Multiple path traversal vulnerability in appspawn and nwebspawn services. Local attackers can create arbitrary directories or escape application sandbox.If chained with other vulnerabilities it would allow an unprivileged process to gain full root privileges. **CVE ID : CVE-2022-43451**	N/A	A-OPE-OPEN-221122/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Files or Directories Accessible to External Parties	03-Nov-2022	5.5	OpenHarmony-v3.1.2 and prior versions had an Arbitrary file read vulnerability via download_server. Local attackers can install an malicious application on the device and reveal any file from the filesystem that is accessible to download_server service which run with UID 1000. **CVE ID : CVE-2022-43449**	N/A	A-OPE-OPEN-221122/750
Vendor: Openssl					
Product: openssl					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	7.5	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker	https://www.openssl.org/news/secadv/20221101.txt, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0023, https://security.netapp.com/advisory/ntap-20221102-0001/	A-OPE-OPEN-221122/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6). **CVE ID : CVE-2022-3602**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	7.5	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the `.' character	https://www.openssl.org/news/secadv/20221101.txt	A-OPE-OPEN-221122/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. **CVE ID : CVE-2022-3786**		
Vendor: Opensuse					
Product: openldap2					
Affected Version(s): * Up to (excluding) 2.6.3-404.1					
Untrusted Search Path	09-Nov-2022	7.8	A Untrusted Search Path vulnerability in openldap2 of openSUSE Factory allows local attackers with control of the ldap user or group to change ownership of arbitrary directory entries to this user/group, leading to escalation to root. This issue affects: openSUSE Factory openldap2 versions prior to 2.6.3-404.1. **CVE ID : CVE-2022-31253**	https://bugzilla.suse.com/show_bug.cgi?id=1202931	A-OPE-OPEN-221122/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: openwrt					
Product: luci					
Affected Version(s): git-22.140.66206-02913be					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	OpenWRT LuCI version git-22.140.66206-02913be was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component /system/sshkeys.js. This vulnerability allows attackers to execute arbitrary web scripts or HTML via crafted public key comments. **CVE ID : CVE-2022-41435**	https://github.com/openwrt/luci/commit/944b55738e7f9685865d5298248b7fbd7380749e	A-OPE-LUCI-221122/754
Vendor: openzeppelin					
Product: contracts					
Affected Version(s): From (including) 3.2.0 Up to (excluding) 4.4.1					
Improper Initialization	04-Nov-2022	5.6	OpenZeppelin Contracts is a library for secure smart contract development. Before version 4.4.1 but after 3.2.0, initializer functions that are invoked separate from contract creation (the most prominent example being minimal proxies) may be reentered if they	https://github.com/OpenZeppelin/openzeppelin-contracts/pull/3006, https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-9c22-pwxw-p6hx	A-OPE-CONT-221122/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make an untrusted non-view external call. Once an initializer has finished running it can never be re-executed. However, an exception put in place to support multiple inheritance made reentrancy possible in the scenario described above, breaking the expectation that there is a single execution. Note that upgradeable proxies are commonly initialized together with contract creation, where reentrancy is not feasible, so the impact of this issue is believed to be minor. This issue has been patched, please upgrade to version 4.4.1. As a workaround, avoid untrusted external calls during initialization. **CVE ID : CVE-2022-39384**		
Product: contracts-upgradeable					
Affected Version(s): From (including) 3.2.0 Up to (excluding) 4.4.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	04-Nov-2022	5.6	OpenZeppelin Contracts is a library for secure smart contract development. Before version 4.4.1 but after 3.2.0, initializer functions that are invoked separate from contract creation (the most prominent example being minimal proxies) may be reentered if they make an untrusted non-view external call. Once an initializer has finished running it can never be re-executed. However, an exception put in place to support multiple inheritance made reentrancy possible in the scenario described above, breaking the expectation that there is a single execution. Note that upgradeable proxies are commonly initialized together with contract creation, where reentrancy is not feasible, so the impact of this issue is believed to be	https://github.com/OpenZeppelin/openzeppelin-contracts/pull/3006, https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-9c22-pwxw-p6hx	A-OPE-CONT-221122/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			minor. This issue has been patched, please upgrade to version 4.4.1. As a workaround, avoid untrusted external calls during initialization. **CVE ID : CVE-2022-39384**		
Vendor: opmc					
Product: woocommerce_dropshipping					
Affected Version(s): * Up to (excluding) 4.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Nov-2022	9.8	The WooCommerce Dropshipping WordPress plugin before 4.4 does not properly sanitise and escape a parameter before using it in a SQL statement via a REST endpoint available to unauthenticated users, leading to a SQL injection **CVE ID : CVE-2022-3481**	https://wpscan.com/vulnerability/c5e395f8-257e-49eb-afbd-9c1e26045373	A-OPM-WOOC-221122/757
Vendor: Oracle					
Product: restaurant_menu_-_food_ordering_system_-_table_reservation					
Affected Version(s): * Up to (excluding) 2.3.1					
Missing Authorization	03-Nov-2022	6.5	The Restaurant Menu – Food Ordering System – Table Reservation plugin for WordPress is vulnerable to authorization bypass via several	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2793398%40menu-ordering-	A-ORA-REST-221122/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AJAX actions in versions up to, and including 2.3.0 due to missing capability checks and missing nonce validation. This makes it possible for authenticated attackers with minimal permissions to perform a wide variety of actions such as modifying the plugin's settings and modifying the ordering system preferences. **CVE ID : CVE-2022-2696**	reservations&new=2793398%40menu-ordering-reservations&sfp_email=&sfph_mail=	
Affected Version(s): * Up to (excluding) 2.3.2					
Cross-Site Request Forgery (CSRF)	03-Nov-2022	8.8	The Restaurant Menu – Food Ordering System – Table Reservation plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.3.1. This is due to missing or incorrect nonce validation on several functions called via AJAX actions such as forms_action, set_option, & chosen_options to	N/A	A-ORA-REST-221122/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name a few . This makes it possible for unauthenticated attackers to perform a variety of administrative actions like modifying forms, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2022-3776**		
Vendor: osisoft-pi-web-connector_project					
Product: osisoft-pi-web-connector					
Affected Version(s): From (including) 0.15.0 Up to (excluding) 0.44.0					
Insertion of Sensitive Information into Log File	04-Nov-2022	4.2	The Foundry Magritte plugin osisoft-pi-web-connector versions 0.15.0 - 0.43.0 was found to be logging in a manner that captured authentication requests. This vulnerability is resolved in osisoft-pi-web-connector version 0.44.0. **CVE ID : CVE-2022-27893**	https://github.com/palantir/security-bulletins/blob/main/PLTRSEC-2022-03.md	A-OSI-OSIS-221122/760
Vendor: Owncloud					
Product: owncloud					
Affected Version(s): * Up to (including) 10.11.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Nov-2022	5.3	The Docker image of ownCloud Server through 10.11 contains a misconfiguration that renders the trusted_domains config useless. This could be abused to spoof the URL in password-reset e-mail messages. **CVE ID : CVE-2022-43679**	https://owncloud.com	A-OWN-OWNC-221122/761
Vendor: palantir					
Product: foundry_blobster					
Affected Version(s): From (including) 3.207.0 Up to (excluding) 3.227.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	5.4	The Foundry Blobster service was found to have a cross-site scripting (XSS) vulnerability that could have allowed an attacker with access to Foundry to launch attacks against other users. This vulnerability is resolved in Blobster 3.228.0. **CVE ID : CVE-2022-27894**	N/A	A-PAL-FOUN-221122/762
Vendor: Paloaltonetworks					
Product: cortex_xsoar					
Affected Version(s): 6.5.0					
Insufficient Verification of Data	09-Nov-2022	6.7	A local privilege escalation (PE) vulnerability in the Palo Alto Networks Cortex XSOAR	https://security.paloaltonetworks.com/C	A-PAL-CORT-221122/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			engine software running on a Linux operating system allows a local attacker with shell access to the engine to execute programs with elevated privileges. **CVE ID : CVE-2022-0031**	VE-2022-0031	
Affected Version(s): 6.6.0					
Insufficient Verification of Data Authenticity	09-Nov-2022	6.7	A local privilege escalation (PE) vulnerability in the Palo Alto Networks Cortex XSOAR engine software running on a Linux operating system allows a local attacker with shell access to the engine to execute programs with elevated privileges. **CVE ID : CVE-2022-0031**	https://security.paloaltonetworks.com/CVE-2022-0031	A-PAL-CORT-221122/764
Affected Version(s): 6.8.0					
Insufficient Verification of Data Authenticity	09-Nov-2022	6.7	A local privilege escalation (PE) vulnerability in the Palo Alto Networks Cortex XSOAR engine software running on a Linux operating system allows a local attacker with shell access to the engine to execute	https://security.paloaltonetworks.com/CVE-2022-0031	A-PAL-CORT-221122/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			programs with elevated privileges. **CVE ID : CVE-2022-0031**		
Vendor: parseplatform					
Product: parse-server					
Affected Version(s): * Up to (excluding) 4.10.18					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	10-Nov-2022	9.8	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 4.10.18, and prior to 5.3.1 on the 5.X branch, are vulnerable to Remote Code Execution via prototype pollution. An attacker can use this prototype pollution sink to trigger a remote code execution through the MongoDB BSON parser. This issue is patched in version 5.3.1 and in 4.10.18. There are no known workarounds. **CVE ID : CVE-2022-39396**	https://github.com/parse-community/parse-server/security/advisories/GHSA-prm5-8g2m-24gg	A-PAR-PARS-221122/766
Affected Version(s): * Up to (excluding) 4.10.19					
Improperly Controlled Modificatio	10-Nov-2022	9.8	Parse Server is an open source backend that can be	https://github.com/parse-community/p	A-PAR-PARS-221122/767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n of Object Prototype Attributes ('Prototype Pollution')			deployed to any infrastructure that can run Node.js. In versions prior to 5.3.2 or 4.10.19, keywords that are specified in the Parse Server option `requestKeywordDenylist` can be injected via Cloud Code Webhooks or Triggers. This will result in the keyword being saved to the database, bypassing the `requestKeywordDenylist` option. This issue is fixed in versions 4.10.19, and 5.3.2. If upgrade is not possible, the following Workarounds may be applied: Configure your firewall to only allow trusted servers to make request to the Parse Server Cloud Code Webhooks API, or block the API completely if you are not using the feature. **CVE ID : CVE-2022-41878**	arse-server/security/advisories/GHSA-xprv-wvh7-qqqx	
Affected Version(s): * Up to (excluding) 4.10.20					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	10-Nov-2022	9.8	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 5.3.3 or 4.10.20, a compromised Parse Server Cloud Code Webhook target endpoint allows an attacker to use prototype pollution to bypass the Parse Server `requestKeywordDenylist` option. This issue has been patched in versions 5.3.3 and 4.10.20. There are no known workarounds. **CVE ID : CVE-2022-41879**	https://github.com/parse-community/parse-server/security/advisories/GHSA-93vw-8fm5-p2jf	A-PAR-PARS-221122/768
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.3.1					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	10-Nov-2022	9.8	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 4.10.18, and prior to 5.3.1 on the 5.X branch, are vulnerable to Remote Code Execution via prototype pollution. An attacker can use	https://github.com/parse-community/parse-server/security/advisories/GHSA-prm5-8g2m-24gg	A-PAR-PARS-221122/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this prototype pollution sink to trigger a remote code execution through the MongoDB BSON parser. This issue is patched in version 5.3.1 and in 4.10.18. There are no known workarounds. **CVE ID : CVE-2022-39396**		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.3.2					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	10-Nov-2022	9.8	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 5.3.2 or 4.10.19, keywords that are specified in the Parse Server option `requestKeywordDenylist` can be injected via Cloud Code Webhooks or Triggers. This will result in the keyword being saved to the database, bypassing the `requestKeywordDenylist` option. This issue is fixed in versions 4.10.19, and 5.3.2. If upgrade is not possible, the	https://github.com/parse-community/parse-server/security/advisories/GHSA-xprv-wvh7-qqqx	A-PAR-PARS-221122/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			following Workarounds may be applied: Configure your firewall to only allow trusted servers to make request to the Parse Server Cloud Code Webhooks API, or block the API completely if you are not using the feature. **CVE ID : CVE-2022-41878**		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.3.3					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	10-Nov-2022	9.8	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 5.3.3 or 4.10.20, a compromised Parse Server Cloud Code Webhook target endpoint allows an attacker to use prototype pollution to bypass the Parse Server `requestKeywordDenylist` option. This issue has been patched in versions 5.3.3 and 4.10.20. There are no known workarounds.	https://github.com/parse-community/parse-server/security/advisories/GHSA-93vw-8fm5-p2jf	A-PAR-PARS-221122/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41879		
Vendor: passwork					
Product: passwork					
Affected Version(s): 5.0.9					
Cleartext Storage of Sensitive Information	07-Nov-2022	7.5	The PassWork extension 5.0.9 for Chrome and other browsers allows an attacker to obtain cleartext cached credentials. **CVE ID : CVE-2022-42955**	https://passwork.canny.io/changelog/version-5110	A-PAS-PASS-221122/772
Cleartext Storage of Sensitive Information	07-Nov-2022	7.5	The PassWork extension 5.0.9 for Chrome and other browsers allows an attacker to obtain the cleartext master password. **CVE ID : CVE-2022-42956**	https://passwork.canny.io/changelog/version-5110	A-PAS-PASS-221122/773
Vendor: pattersondental					
Product: eaglesoft					
Affected Version(s): 21.0					
Use of Hard-coded Credentials	07-Nov-2022	7.8	Patterson Dental Eaglesoft 21 has AES-256 encryption but there are two ways to obtain a keyfile: (1) keybackup.data > License > Encryption Key or (2) Eaglesoft.Server.Configuration.data > DbEncryptKeyPrimary > Encryption	N/A	A-PAT-EAGL-221122/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Key. Applicable files are encrypted with keys and salt that are hardcoded into a DLL or EXE file. **CVE ID : CVE-2022-37710**		
Vendor: payara					
Product: payara					
Affected Version(s): * Up to (excluding) 4.1.2.191.38					
Files or Directories Accessible to External Parties	10-Nov-2022	7.5	Payara before 2022-11-04, when deployed to the root context, allows attackers to visit META-INF and WEB-INF, a different vulnerability than CVE-2022-37422. This affects Payara Platform Community before 4.1.2.191.38, 5.x before 5.2022.4, and 6.x before 6.2022.1, and Payara Platform Enterprise before 5.45.0. **CVE ID : CVE-2022-45129**	https://github.com/payara/Payara/commit/cccdfddeda71c78ae7b3179db5429e1bb8a56b2e, https://docs.payara.fish/community/docs/Release%20Notes/Release%20Notes%205.2022.4.html, https://blog.payara.fish/whats-new-in-the-november-2022-payara-platform-release	A-PAY-PAYA-221122/775
Affected Version(s): * Up to (excluding) 5.45.0					
Files or Directories Accessible to External Parties	10-Nov-2022	7.5	Payara before 2022-11-04, when deployed to the root context, allows attackers to visit META-INF and WEB-INF, a	https://github.com/payara/Payara/commit/cccdfddeda71c78ae7b3179db5429e1bb8a56b2e,	A-PAY-PAYA-221122/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different vulnerability than CVE-2022-37422. This affects Payara Platform Community before 4.1.2.191.38, 5.x before 5.2022.4, and 6.x before 6.2022.1, and Payara Platform Enterprise before 5.45.0. **CVE ID : CVE-2022-45129**	https://docs.payara.fish/community/docs/Release%20Notes/Release%20Notes%205.2022.4.html, https://blog.payara.fish/whats-new-in-the-november-2022-payara-platform-release	
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.2022.4					
Files or Directories Accessible to External Parties	10-Nov-2022	7.5	Payara before 2022-11-04, when deployed to the root context, allows attackers to visit META-INF and WEB-INF, a different vulnerability than CVE-2022-37422. This affects Payara Platform Community before 4.1.2.191.38, 5.x before 5.2022.4, and 6.x before 6.2022.1, and Payara Platform Enterprise before 5.45.0. **CVE ID : CVE-2022-45129**	https://github.com/payara/Payara/commit/cccdfddeda71c78ae7b3179db5429e1bb8a56b2e, https://docs.payara.fish/community/docs/Release%20Notes/Release%20Notes%205.2022.4.html, https://blog.payara.fish/whats-new-in-the-november-2022-payara-platform-release	A-PAY-PAYA-221122/777
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.2022.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Files or Directories Accessible to External Parties	10-Nov-2022	7.5	Payara before 2022-11-04, when deployed to the root context, allows attackers to visit META-INF and WEB-INF, a different vulnerability than CVE-2022-37422. This affects Payara Platform Community before 4.1.2.191.38, 5.x before 5.2022.4, and 6.x before 6.2022.1, and Payara Platform Enterprise before 5.45.0. **CVE ID : CVE-2022-45129**	https://github.com/payara/Payara/commit/cccdfddeda71c78ae7b3179db5429e1bb8a56b2e, https://docs.payara.fish/community/docs/Release%20Notes/Release%20Notes%205.2022.4.html, https://blog.payara.fish/whats-new-in-the-november-2022-payara-platform-release	A-PAY-PAYA-221122/778
Vendor: pdfhummus					
Product: hummusjs					
Affected Version(s): * Up to (excluding) 1.0.111					
NULL Pointer Dereference	02-Nov-2022	5.5	Muhammara is a node module with c/cpp bindings to modify PDF with js for node or electron (based/replacement on/of galkhana/hummusjs). The package muhammara before 2.6.0; all versions of package hummus are vulnerable to Denial of Service (DoS) when supplied with a maliciously crafted	https://github.com/julianhille/MuhammaraJS/security/advisories/GHSA-rcrx-fpjp-mfrw, https://github.com/julianhille/MuhammaraJS/pull/194	A-PDF-HUMM-221122/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PDF file to be appended to another. This issue has been patched in 2.6.0 for muhammara and not at all for hummus. As a workaround, do not process files from untrusted sources. **CVE ID : CVE-2022-39381**		
Vendor: PHP					
Product: php					
Affected Version(s): * Up to (excluding) 7.4.33					
Out-of-bounds Read	14-Nov-2022	7.1	In PHP versions prior to 7.4.33, 8.0.25 and 8.2.12, when using imageloadfont() function in gd extension, it is possible to supply a specially crafted font file, such as if the loaded font is used with imagechar() function, the read outside allocated buffer will be used. This can lead to crashes or disclosure of confidential information. **CVE ID : CVE-2022-31630**	https://bugs.php.net/bug.php?id=81739	A-PHP-PHP-221122/780
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.25					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	14-Nov-2022	7.1	In PHP versions prior to 7.4.33, 8.0.25 and 8.2.12, when using imageloadfont() function in gd extension, it is possible to supply a specially crafted font file, such as if the loaded font is used with imagechar() function, the read outside allocated buffer will be used. This can lead to crashes or disclosure of confidential information. **CVE ID : CVE-2022-31630**	https://bugs.php.net/bug.php?id=81739	A-PHP-PHP-221122/781
Affected Version(s): From (including) 8.2.0 Up to (excluding) 8.2.12					
Out-of-bounds Read	14-Nov-2022	7.1	In PHP versions prior to 7.4.33, 8.0.25 and 8.2.12, when using imageloadfont() function in gd extension, it is possible to supply a specially crafted font file, such as if the loaded font is used with imagechar() function, the read outside allocated buffer will be used. This can lead to crashes or disclosure of	https://bugs.php.net/bug.php?id=81739	A-PHP-PHP-221122/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidential information. **CVE ID : CVE-2022-31630**		
Vendor: Phpipam					
Product: phpipam					
Affected Version(s): * Up to (excluding) 1.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	6.1	A vulnerability has been found in phpipam and classified as problematic. Affected by this vulnerability is an unknown functionality of the file app/admin/import-export/import-load-data.php of the component Import Preview Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.5.0 is able to address this issue. The name of the patch is 22c797c3583001211fe7d31bccd3f1d4aeeb3bbc. It is recommended to upgrade the affected component. The associated identifier of this	https://github.com/phpipam/phpipam/commit/22c797c3583001211fe7d31bccd3f1d4aeeb3bbc	A-PHP-PHPI-221122/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-212863. **CVE ID : CVE-2022-3845**		
Vendor: picoc_project					
Product: picoc					
Affected Version(s): 3.2.2					
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the ExpressionCoerceInteger function in expression.c when called from ExpressionInfixOperator. **CVE ID : CVE-2022-44312**	N/A	A-PIC-PICO-221122/784
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the ExpressionCoerceUnsignedInteger function in expression.c when called from ExpressionParseFunctionCall. **CVE ID : CVE-2022-44313**	N/A	A-PIC-PICO-221122/785
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StringStrncpy function in cstdlib/string.c	N/A	A-PIC-PICO-221122/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when called from ExpressionParseFunctionCall. **CVE ID : CVE-2022-44314**		
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the ExpressionAssign function in expression.c when called from ExpressionParseFunctionCall. **CVE ID : CVE-2022-44315**	N/A	A-PIC-PICO-221122/787
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the LexGetStringConstant function in lex.c when called from LexScanGetToken. **CVE ID : CVE-2022-44316**	N/A	A-PIC-PICO-221122/788
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StdioOutPutc function in cstdlib/stdio.c when called from ExpressionParseFunctionCall. **CVE ID : CVE-2022-44317**	N/A	A-PIC-PICO-221122/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StringStrcat function in cstdlib/string.c when called from ExpressionParseFunctionCall. **CVE ID : CVE-2022-44318**	N/A	A-PIC-PICO-221122/790
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StdioBasePrintf function in cstdlib/string.c when called from ExpressionParseFunctionCall. **CVE ID : CVE-2022-44319**	N/A	A-PIC-PICO-221122/791
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the ExpressionCoerceFP function in expression.c when called from ExpressionParseFunctionCall. **CVE ID : CVE-2022-44320**	N/A	A-PIC-PICO-221122/792
Out-of-bounds Write	08-Nov-2022	5.5	PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the	N/A	A-PIC-PICO-221122/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LexSkipComment function in lex.c when called from LexScanGetToken. **CVE ID : CVE-2022-44321**		
Vendor: pingcap					
Product: tidb					
Affected Version(s): * Up to (excluding) 6.4.0					
Use of Externally-Controlled Format String	04-Nov-2022	9.8	Use of Externally-Controlled Format String in GitHub repository pingcap/tidb prior to 6.4.0, 6.1.3. **CVE ID : CVE-2022-3023**	https://huntr.dev/bounties/120f1346-e958-49d0-b66c-0f889a469540, https://github.com/pingcap/tidb/commit/d0376379d615cc8f263a0b17c031ce403c8dcbfb	A-PIN-TIDB-221122/794
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.3					
Use of Externally-Controlled Format String	04-Nov-2022	9.8	Use of Externally-Controlled Format String in GitHub repository pingcap/tidb prior to 6.4.0, 6.1.3. **CVE ID : CVE-2022-3023**	https://huntr.dev/bounties/120f1346-e958-49d0-b66c-0f889a469540, https://github.com/pingcap/tidb/commit/d0376379d615cc8f263a0b17c031ce403c8dcbfb	A-PIN-TIDB-221122/795
Vendor: pistar					
Product: pi-star_digital_voice_dashboard					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2022-10-03					
N/A	11-Nov-2022	9.8	Pi-Star_DV_Dash (for Pi-Star DV) before 5aa194d mishandles the module parameter. **CVE ID : CVE-2022-45182**	https://github.com/AndyTaylorTweet/Pi-Star_DV_Dash/commit/0ad7d00210fc2c0eb7073e5ed429ac265ccfebbd, https://github.com/AndyTaylorTweet/Pi-Star_DV_Dash/commit/5aa194df3dfc92cc21f6604bbda32268f4a624ce, https://www.pistar.uk/	A-PIS-PI-S-221122/796
Vendor: Pixman					
Product: pixman					
Affected Version(s): * Up to (excluding) 0.42.2					
Integer Overflow or Wraparound	03-Nov-2022	8.8	In libpixman in Pixman before 0.42.2, there is an out-of-bounds write (aka heap-based buffer overflow) in rasterize_edges_8 due to an integer overflow in pixman_sample_floor_y. **CVE ID : CVE-2022-44638**	https://gitlab.freedesktop.org/pixman/pixman/-/issues/63	A-PIX-PIXM-221122/797
Vendor: Plesk					
Product: obsidian					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	10-Nov-2022	6.5	Plesk Obsidian allows a CSRF attack, e.g., via the /api/v2/cli/commands REST API to change an Admin password. NOTE: Obsidian is a specific version of the Plesk product: version numbers were used through version 12, and then the convention was changed so that versions are identified by names ("Obsidian"), not numbers. **CVE ID : CVE-2022-45130**	https://fortbridge.co.uk/research/compromising-plesk-via-its-rest-api/	A-PLE-OBSI-221122/798
Vendor: publiccms					
Product: publiccms					
Affected Version(s): * Up to (excluding) 2022-09-14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	6.1	A vulnerability, which was classified as problematic, was found in sanluan PublicCMS. Affected is the function initLink of the file dwz.min.js of the component Tab Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is	https://github.com/sanluan/PublicCMS/commit/a972dc9b1c94aea2d84478bf26283904c21e4ca2	A-PUB-PUBL-221122/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a972dc9b1c94aea2d84478bf26283904c21e4ca2. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-213456. **CVE ID : CVE-2022-3950**		
Vendor: pymatgen					
Product: pymatgen					
Affected Version(s): -					
N/A	09-Nov-2022	7.5	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the pymatgen PyPI package, when an attacker is able to supply arbitrary input to the GaussianInput.from_string method **CVE ID : CVE-2022-42964**	N/A	A-PYM-PYMA-221122/800
Vendor: Python					
Product: pillow					
Affected Version(s): * Up to (excluding) 9.2.0					
N/A	14-Nov-2022	7.5	Pillow before 9.2.0 performs Improper Handling of Highly Compressed GIF Data (Data Amplification). **CVE ID : CVE-2022-45198**	https://github.com/python-pillow/Pillow/commit/11918eac0628ec8ac0812670d9838361ead2d6a4, https://github.com/python-	A-PYT-PILL-221122/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				pillow/Pillow/pull/6402	
Affected Version(s): * Up to (excluding) 9.3.0					
Uncontrolled Resource Consumption	14-Nov-2022	7.5	Pillow before 9.3.0 allows denial of service via SAMPLESPERPIXEL. **CVE ID : CVE-2022-45199**	https://github.com/python-pillow/Pillow/pull/6700, https://github.com/python-pillow/Pillow/commit/2444cddab2f83f28687c7c20871574acbb6dbcf3	A-PYT-PILL-221122/802
Product: python					
Affected Version(s): * Up to (including) 3.7.15					
Uncontrolled Resource Consumption	09-Nov-2022	7.5	An issue was discovered in Python before 3.11.1. An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service. Hostnames are often supplied by remote servers that could be controlled by a malicious actor; in such a scenario, they could trigger	https://github.com/python/cpython/issues/98433	A-PYT-PYTH-221122/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			excessive CPU consumption on the client attempting to make use of an attacker-supplied supposed hostname. For example, the attack payload could be placed in the Location header of an HTTP response with status code 302. A fix is planned in 3.11.1, 3.10.9, 3.9.16, 3.8.16, and 3.7.16. **CVE ID : CVE-2022-45061**		
Affected Version(s): 3.11.0					
Uncontrolled Resource Consumption	09-Nov-2022	7.5	An issue was discovered in Python before 3.11.1. An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service. Hostnames are often supplied by remote servers that could be controlled by a malicious actor; in	https://github.com/python/cpython/issues/98433	A-PYT-PYTH-221122/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such a scenario, they could trigger excessive CPU consumption on the client attempting to make use of an attacker-supplied supposed hostname. For example, the attack payload could be placed in the Location header of an HTTP response with status code 302. A fix is planned in 3.11.1, 3.10.9, 3.9.16, 3.8.16, and 3.7.16. **CVE ID : CVE-2022-45061**		
Affected Version(s): From (including) 3.10.0 Up to (including) 3.10.8					
Uncontrolled Resource Consumption	09-Nov-2022	7.5	An issue was discovered in Python before 3.11.1. An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service. Hostnames are often supplied by remote servers that could be	https://github.com/python/cpython/issues/98433	A-PYT-PYTH-221122/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlled by a malicious actor; in such a scenario, they could trigger excessive CPU consumption on the client attempting to make use of an attacker-supplied supposed hostname. For example, the attack payload could be placed in the Location header of an HTTP response with status code 302. A fix is planned in 3.11.1, 3.10.9, 3.9.16, 3.8.16, and 3.7.16. **CVE ID : CVE-2022-45061**		
Affected Version(s): From (including) 3.8.0 Up to (including) 3.8.15					
Uncontrolled Resource Consumption	09-Nov-2022	7.5	An issue was discovered in Python before 3.11.1. An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service. Hostnames are often supplied	https://github.com/python/cpython/issues/98433	A-PYT-PYTH-221122/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by remote servers that could be controlled by a malicious actor; in such a scenario, they could trigger excessive CPU consumption on the client attempting to make use of an attacker-supplied supposed hostname. For example, the attack payload could be placed in the Location header of an HTTP response with status code 302. A fix is planned in 3.11.1, 3.10.9, 3.9.16, 3.8.16, and 3.7.16. **CVE ID : CVE-2022-45061**		
Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.10.8					
N/A	07-Nov-2022	7.8	Python 3.9.x and 3.10.x through 3.10.8 on Linux allows local privilege escalation in a non-default configuration. The Python multiprocessing library, when used with the forkserver start method on Linux, allows pickles to be deserialized from any user in the same machine local	N/A	A-PYT-PYTH-221122/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network namespace, which in many system configurations means any user on the same machine. Pickles can execute arbitrary code. Thus, this allows for local user privilege escalation to the user that any forkserver process is running as. Setting multiprocessing.util.abstract_sockets_supported to False is a workaround. The forkserver start method for multiprocessing is not the default start method. This issue is Linux specific because only Linux supports abstract namespace sockets. CPython before 3.9 does not make use of Linux abstract namespace sockets by default. Support for users manually specifying an abstract namespace socket was added as a bugfix in 3.7.8 and 3.8.4, but users would need to make specific uncommon API calls in order to do		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that in CPython before 3.9. **CVE ID : CVE-2022-42919**		
Affected Version(s): From (including) 3.9.0 Up to (including) 3.9.15					
Uncontrolled Resource Consumption	09-Nov-2022	7.5	An issue was discovered in Python before 3.11.1. An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service. Hostnames are often supplied by remote servers that could be controlled by a malicious actor; in such a scenario, they could trigger excessive CPU consumption on the client attempting to make use of an attacker-supplied supposed hostname. For example, the attack payload could be placed in the Location header of an HTTP response with status code	https://github.com/python/cpython/issues/98433	A-PYT-PYTH-221122/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			302. A fix is planned in 3.11.1, 3.10.9, 3.9.16, 3.8.16, and 3.7.16. **CVE ID : CVE-2022-45061**		
Vendor: python-poetry					
Product: cleo					
Affected Version(s): -					
N/A	09-Nov-2022	7.5	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the cleo PyPI package, when an attacker is able to supply arbitrary input to the Table.set_rows method **CVE ID : CVE-2022-42966**	N/A	A-PYT-CLEO-221122/809
Vendor: Qemu					
Product: qemu					
Affected Version(s): 7.1.0					
Off-by-one Error	07-Nov-2022	8.6	An off-by-one read/write issue was found in the SDHCI device of QEMU. It occurs when reading/writing the Buffer Data Port Register in sdhci_read_dataport and sdhci_write_dataport, respectively, if data_count == block_size. A malicious guest	https://lists.nongnu.org/archive/html/qemu-devel/2022-11/msg01068.html	A-QEM-QEMU-221122/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition. **CVE ID : CVE-2022-3872**		
Affected Version(s): * Up to (excluding) 7.1.0					
Off-by-one Error	07-Nov-2022	8.6	An off-by-one read/write issue was found in the SDHCI device of QEMU. It occurs when reading/writing the Buffer Data Port Register in sdhci_read_dataport and sdhci_write_dataport, respectively, if data_count == block_size. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition. **CVE ID : CVE-2022-3872**	https://lists.nongnu.org/archive/html/qemu-devel/2022-11/msg01068.html	A-QEM-QEMU-221122/811
Vendor: really-simple-plugins					
Product: complianz					
Affected Version(s): * Up to (excluding) 6.3.4					
Improper Neutralization of Special Elements	07-Nov-2022	8.8	The Complianz WordPress plugin before 6.3.4, and Complianz Premium	https://wpscan.com/vulnerability/71db75c0-5907-4237-884f-	A-REA-COMP-221122/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			WordPress plugin before 6.3.6 allow a translators to inject arbitrary SQL through an unsanitized translation. SQL can be injected through an infected translation file, or by a user with a translator role through translation plugins such as Loco Translate or WPML. **CVE ID : CVE-2022-3494**	8db88b1a9b34	
Affected Version(s): * Up to (excluding) 6.3.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Nov-2022	8.8	The Complianz WordPress plugin before 6.3.4, and Complianz Premium WordPress plugin before 6.3.6 allow a translators to inject arbitrary SQL through an unsanitized translation. SQL can be injected through an infected translation file, or by a user with a translator role through translation plugins such as Loco Translate or WPML. **CVE ID : CVE-2022-3494**	https://wpscan.com/vulnerability/71db75c0-5907-4237-884f-8db88b1a9b34	A-REA-COMP-221122/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Redhat					
Product: fedora_coreos					
Affected Version(s): From (including) 36.20220820.3.0 Up to (excluding) 37.20221031.1.0					
Missing Authorization	03-Nov-2022	5.5	Fedora CoreOS supports setting a GRUB bootloader password using a Butane config. When this feature is enabled, GRUB requires a password to access the GRUB command-line, modify kernel command-line arguments, or boot non-default OSTree deployments. Recent Fedora CoreOS releases have a misconfiguration which allows booting non-default OSTree deployments without entering a password. This allows someone with access to the GRUB menu to boot into an older version of Fedora CoreOS, reverting any security fixes that have recently been applied to the machine. A password is still required to modify kernel command-line arguments and	https://docs.fedoraproject.org/en-US/fedora-coreos/grub-password/, https://lists.fedoraproject.org/archives/list/coreos-status@lists.fedoraproject.org/thread/NHUCNH5Y4UH5DPUCXISYXXVA563TLFEJ/	A-RED-FEDO-221122/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the GRUB command line. **CVE ID : CVE-2022-3675**		
Product: openshift_container_platform					
Affected Version(s): -					
Exposure of Resource to Wrong Sphere	03-Nov-2022	3.3	"IBM Robotic Process Automation for Cloud Pak 21.0.1, 21.0.2, 21.0.3, 21.0.4, and 21.0.5 is vulnerable to exposure of the first tenant owner e-mail address to users with access to the container platform. IBM X-Force ID: 238214." **CVE ID : CVE-2022-42442**	https://www.ibm.com/support/pages/node/6831787	A-RED-OPEN-221122/815
Vendor: resmush.it					
Product: resmush.it_image_optimizer					
Affected Version(s): * Up to (excluding) 0.4.4					
Missing Authorization	14-Nov-2022	4.3	The reSmush.it : the only free Image Optimizer & compress plugin WordPress plugin before 0.4.4 lacks authorization in various AJAX actions, allowing any logged-in users, such as subscribers to call them. **CVE ID : CVE-2022-2450**	https://wpscan.com/vulnerability/1b3ff124-f973-4584-a7d7-26cc404bfe2b	A-RES-RESM-221122/816
Affected Version(s): * Up to (excluding) 0.4.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	14-Nov-2022	6.5	The reSmush.it : the only free Image Optimizer & compress plugin WordPress plugin before 0.4.4 does not perform CSRF checks for any of its AJAX actions, allowing an attackers to trick logged in users to perform various actions on their behalf on the site. **CVE ID : CVE-2022-2449**	https://wpscan.com/vulnerability/6e42f26b-3403-4d55-99ad-2c8e2d76e537	A-RES-RESM-221122/817
Vendor: restaurant_pos_system_project					
Product: restaurant_pos_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	01-Nov-2022	7.2	An arbitrary file upload vulnerability in add_product.php of Restaurant POS System v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-43085**	N/A	A-RES-REST-221122/818
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	4.9	Restaurant POS System v1.0 was discovered to contain a SQL injection vulnerability via update_customer.php. **CVE ID : CVE-2022-43086**	N/A	A-RES-REST-221122/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: rockcontent					
Product: rock_convert					
Affected Version(s): * Up to (including) 2.11.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Stage Rock Convert plugin <= 2.11.0 on WordPress. **CVE ID : CVE-2022-36428**	https://wordpress.org/plugins/rock-convert/, https://patchstack.com/database/vulnerability/rock-convert/wordpress-rock-convert-plugin-2-11-0-auth-cross-site-scripting-xss-vulnerability?_s_id=cve	A-ROC-ROCK-221122/820
Vendor: roxyfileman					
Product: roxy_fileman					
Affected Version(s): 1.4.6					
Unrestricted Upload of File with Dangerous Type	09-Nov-2022	9.8	Roxy Fileman 1.4.6 allows Remote Code Execution via a .phar upload, because the default FORBIDDEN_UPLOADS value in conf.json only blocks .php, .php4, and .php5 files. (Visiting any .phar file invokes the PHP interpreter in some realistic web-server configurations.) **CVE ID : CVE-2022-40797**	N/A	A-ROX-ROXY-221122/821
Vendor: rukovoditel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rukovoditel					
Affected Version(s): 3.2.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Nov-2022	8.8	Rukovoditel v3.2.1 was discovered to contain a SQL injection vulnerability via the order_by parameter at /rukovoditel/index.php?module=logs/view&type=php. **CVE ID : CVE-2022-43288**	N/A	A-RUK-RUKO-221122/822
Vendor: rymera					
Product: advanced_coupons					
Affected Version(s): * Up to (including) 4.5					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Advanced Coupons for WooCommerce Coupons plugin <= 4.5 on WordPress leading to notice dismissal. **CVE ID : CVE-2022-43481**	https://patchstack.com/database/vulnerability/advanced-coupons-for-woocommerce-free/wordpress-advanced-coupons-for-woocommerce-coupons-plugin-4-5-cross-site-request-forgery-csrf-vulnerability?_s_id=cve	A-RYM-ADVA-221122/823
Vendor: salonerp_project					
Product: salonerp					
Affected Version(s): 3.0.2					
Improper Neutralizat	03-Nov-2022	6.1	SalonERP version 3.0.2 allows an	N/A	A-SAL-SALO-221122/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			external attacker to steal the cookie of arbitrary users. This is possible because the application does not correctly validate the page parameter against XSS attacks. **CVE ID : CVE-2022-42753**		
Vendor: Samsung					
Product: billing					
Affected Version(s): * Up to (excluding) 5.0.56.0					
N/A	09-Nov-2022	7.5	Improper Authorization in Samsung Billing prior to version 5.0.56.0 allows attacker to get sensitive information. **CVE ID : CVE-2022-39890**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=11	A-SAM-BILL-221122/825
Product: editor_lite					
Affected Version(s): * Up to (excluding) 4.0.41.3					
Out-of-bounds Write	09-Nov-2022	7.5	Heap overflow vulnerability in parse_pce function in libsavsaudio.so in Editor Lite prior to version 4.0.41.3 allows attacker to get information. **CVE ID : CVE-2022-39891**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=11	A-SAM-EDIT-221122/826
Product: galaxywatch4plugin					
Affected Version(s): * Up to (excluding) 2.2.11.22101351					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	3.3	Improper access control vulnerability in GalaxyWatch4Plugin prior to versions 2.2.11.22101351 and 2.2.12.22101351 allows attackers to access wearable device information. **CVE ID : CVE-2022-39889**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=11	A-SAM-GALA-221122/827
Affected Version(s): 2.2.11.22102751					
N/A	09-Nov-2022	3.3	Improper access control vulnerability in GalaxyWatch4Plugin prior to versions 2.2.11.22101351 and 2.2.12.22101351 allows attackers to access wearable device information. **CVE ID : CVE-2022-39889**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=11	A-SAM-GALA-221122/828
Product: galaxy_buds_pro_manage					
Affected Version(s): * Up to (excluding) 4.1.22092751					
Insertion of Sensitive Information into Log File	09-Nov-2022	3.3	Sensitive information exposure vulnerability in FmmBaseModel in Galaxy Buds Pro Manage prior to version 4.1.22092751 allows local attackers with log access permission to get device	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=11	A-SAM-GALA-221122/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier data through device log. **CVE ID : CVE-2022-39893**		
Product: pass					
Affected Version(s): * Up to (excluding) 4.0.05.1					
N/A	09-Nov-2022	9.8	Improper access control in Samsung Pass prior to version 4.0.05.1 allows attackers to unauthenticated access via keep open feature. **CVE ID : CVE-2022-39892**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=11	A-SAM-PASS-221122/830
Vendor: sandhillsdev					
Product: easy_digital_downloads					
Affected Version(s): * Up to (excluding) 3.0					
Cross-Site Request Forgery (CSRF)	07-Nov-2022	4.3	The Easy Digital Downloads WordPress plugin before 3.0 does not have CSRF check in place when deleting payment history, and does not ensure that the post to be deleted is actually a payment history. As a result, attackers could make a logged in admin delete arbitrary post via a CSRF attack **CVE ID : CVE-2022-2387**	https://wpscan.com/vulnerability/db3c3c78-1724-4791-9ab6-ebb2e8a4c8b8	A-SAN-EASY-221122/831
Vendor: sanitization_management_system_project					
Product: sanitization_management_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	6.1	A vulnerability was found in SourceCodester Sanitization Management System and classified as problematic. This issue affects some unknown processing of the file php-sms/?p=request_quote. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-213449 was assigned to this vulnerability. **CVE ID : CVE-2022-3942**	N/A	A-SAN-SANI-221122/832
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Nov-2022	9.8	A vulnerability classified as critical has been found in SourceCodester Sanitization Management System. Affected is an unknown function of the file /php-sms/classes/Master.php?f=save_quote. The manipulation of the argument id leads to sql injection. It is	N/A	A-SAN-SANI-221122/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-213012. **CVE ID : CVE-2022-3868**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Nov-2022	7.2	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php-sms/classes/Master.php?f=delete_inquiry. **CVE ID : CVE-2022-43350**	N/A	A-SAN-SANI-221122/834
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Nov-2022	7.2	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php-sms/classes/Master.php?f=delete_quote. **CVE ID : CVE-2022-43352**	N/A	A-SAN-SANI-221122/835
N/A	07-Nov-2022	6.5	Sanitization Management System v1.0 was	N/A	A-SAN-SANI-221122/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain an arbitrary file deletion vulnerability via the component /classes/Master.php?f=delete_img. **CVE ID : CVE-2022-43351**		
N/A	01-Nov-2022	0	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=orders/view_order. **CVE ID : CVE-2022-43353**	N/A	A-SAN-SANI-221122/837
N/A	01-Nov-2022	0	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=orders/manage_request. **CVE ID : CVE-2022-43354**	N/A	A-SAN-SANI-221122/838
N/A	01-Nov-2022	0	Sanitization Management System v1.0 was discovered to contain a SQL injection vulnerability via	N/A	A-SAN-SANI-221122/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the id parameter at /php-sms/classes/Master.php?f=delete_service. **CVE ID : CVE-2022-43355**		
Vendor: SAP					
Product: 3d_visual_enterprise_author					
Affected Version(s): 9					
Out-of-bounds Write	08-Nov-2022	7.8	Due to lack of proper memory management, when a victim opens manipulated file received from untrusted sources in SAP 3D Visual Enterprise Author and SAP 3D Visual Enterprise Viewer, Arbitrary Code Execution can be triggered when payload forces:Re-use of dangling pointer which refers to overwritten space in memory. The accessed memory must be filled with code to execute the attack. Therefore, repeated success is unlikely.Stack-based buffer overflow. Since the memory overwritten is random, based on access rights of the	https://launchpad.support.sap.com/#/notes/3263436, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-221122/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory, repeated success is not assured. **CVE ID : CVE-2022-41211**		
Product: 3d_visual_enterprise_viewer					
Affected Version(s): 9					
Out-of-bounds Write	08-Nov-2022	7.8	Due to lack of proper memory management, when a victim opens manipulated file received from untrusted sources in SAP 3D Visual Enterprise Author and SAP 3D Visual Enterprise Viewer, Arbitrary Code Execution can be triggered when payload forces:Re-use of dangling pointer which refers to overwritten space in memory. The accessed memory must be filled with code to execute the attack. Therefore, repeated success is unlikely.Stack-based buffer overflow. Since the memory overwritten is random, based on access rights of the memory, repeated success is not assured.	https://launchpad.support.sap.com/#/notes/3263436, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-3D_V-221122/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41211		
Product: biller_direct					
Affected Version(s): 635					
URL Redirection to Untrusted Site ('Open Redirect')	08-Nov-2022	6.1	SAP Biller Direct allows an unauthenticated attacker to craft a legitimate looking URL. When clicked by an unsuspecting victim, it will use an unsensitized parameter to redirect the victim to a malicious site of the attacker's choosing which can result in disclosure or modification of the victim's information. **CVE ID : CVE-2022-41207**	https://launchpad.support.sap.com/#/notes/3238042, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BILL-221122/842
Affected Version(s): 750					
URL Redirection to Untrusted Site ('Open Redirect')	08-Nov-2022	6.1	SAP Biller Direct allows an unauthenticated attacker to craft a legitimate looking URL. When clicked by an unsuspecting victim, it will use an unsensitized parameter to redirect the victim to a malicious site of the attacker's choosing which can result in disclosure or modification of	https://launchpad.support.sap.com/#/notes/3238042, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BILL-221122/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the victim's information. **CVE ID : CVE-2022-41207**		
Product: businessobjects_business_intelligence					
Affected Version(s): 4.2					
Deserialization of Untrusted Data	08-Nov-2022	8.8	In some workflow of SAP BusinessObjects BI Platform (Central Management Console and BI LaunchPad), an authenticated attacker with low privileges can intercept a serialized object in the parameters and substitute with another malicious serialized object, which leads to deserialization of untrusted data vulnerability. This could highly compromise the Confidentiality, Integrity, and Availability of the system. **CVE ID : CVE-2022-41203**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3243924	A-SAP-BUSI-221122/844
Affected Version(s): 4.3					
Deserialization of Untrusted Data	08-Nov-2022	8.8	In some workflow of SAP BusinessObjects BI Platform (Central Management Console and BI LaunchPad), an	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b	A-SAP-BUSI-221122/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker with low privileges can intercept a serialized object in the parameters and substitute with another malicious serialized object, which leads to deserialization of untrusted data vulnerability. This could highly compromise the Confidentiality, Integrity, and Availability of the system. **CVE ID : CVE-2022-41203**	.html, https://launchpad.support.sap.com/#/notes/3243924	
Product: financial_consolidation					
Affected Version(s): 1010					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.5	Due to insufficient input validation, SAP Financial Consolidation - version 1010, allows an authenticated attacker to inject malicious script when running a common query in the Web Administration Console. On successful exploitation, an attacker can view or modify information causing a limited	https://launchpad.support.sap.com/#/notes/3260708, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-FINA-221122/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact on confidentiality, integrity and availability of the application. **CVE ID : CVE-2022-41258**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	SAP Financial Consolidation - version 1010, does not sufficiently encode user-controlled input which may allow an unauthenticated attacker to inject a web script via a GET request. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2022-41260**	https://launchpad.support.sap.com/#/notes/3260708, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-FINA-221122/847
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	5.4	Due to insufficient input validation, SAP Financial Consolidation - version 1010, allows an authenticated attacker with user privileges to alter current user session. On successful exploitation, the	https://launchpad.support.sap.com/#/notes/3260708, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-FINA-221122/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can view or modify information, causing a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2022-41208**		
Product: gui					
Affected Version(s): 7.70					
Improper Control of Generation of Code ('Code Injection')	08-Nov-2022	6.1	SAP GUI allows an authenticated attacker to execute scripts in the local network. On successful exploitation, the attacker can gain access to registries which can cause a limited impact on confidentiality and high impact on availability of the application. **CVE ID : CVE-2022-41205**	https://launchpad.support.sap.com/#/notes/3237251, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-GUI-221122/849
Product: netweaver_application_server_abap					
Affected Version(s): 750					
Improper Input Validation	08-Nov-2022	6.5	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.	A-SAP-NETW-221122/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delete a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the integrity and availability of the application. **CVE ID : CVE-2022-41214**	sap.com/#/notes/3256571	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	4.9	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to read a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the confidentiality of the application. **CVE ID : CVE-2022-41212**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/851
URL Redirection to Untrusted Site ('Open Redirect')	08-Nov-2022	4.7	SAP NetWeaver ABAP Server and ABAP Platform allows an unauthenticated attacker to redirect users to a malicious site due to	https://launchpad.support.sap.com/#/notes/3251202, https://www.sap.com/documents/2022/02/fa865ea4-	A-SAP-NETW-221122/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient URL validation. This could lead to the user being tricked to disclose personal information. **CVE ID : CVE-2022-41215**	167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 700					
Improper Input Validation	08-Nov-2022	6.5	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to delete a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the integrity and availability of the application. **CVE ID : CVE-2022-41214**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/853
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	4.9	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.	A-SAP-NETW-221122/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the confidentiality of the application. **CVE ID : CVE-2022-41212**	sap.com/#/notes/3256571	
URL Redirection to Untrusted Site ('Open Redirect')	08-Nov-2022	4.7	SAP NetWeaver ABAP Server and ABAP Platform allows an unauthenticated attacker to redirect users to a malicious site due to insufficient URL validation. This could lead to the user being tricked to disclose personal information. **CVE ID : CVE-2022-41215**	https://launchpad.support.sap.com/#/notes/3251202, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-221122/855
Affected Version(s): 731					
Improper Input Validation	08-Nov-2022	6.5	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to delete a file which is otherwise restricted. On	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploitation an attacker can completely compromise the integrity and availability of the application. **CVE ID : CVE-2022-41214**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	4.9	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to read a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the confidentiality of the application. **CVE ID : CVE-2022-41212**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/857
URL Redirection to Untrusted Site ('Open Redirect')	08-Nov-2022	4.7	SAP NetWeaver ABAP Server and ABAP Platform allows an unauthenticated attacker to redirect users to a malicious site due to insufficient URL validation. This could lead to the	https://launchpad.support.sap.com/#/notes/3251202, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-NETW-221122/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user being tricked to disclose personal information. **CVE ID : CVE-2022-41215**	c68f7e60039b.html	
Affected Version(s): 740					
Improper Input Validation	08-Nov-2022	6.5	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to delete a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the integrity and availability of the application. **CVE ID : CVE-2022-41214**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/859
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	4.9	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to read a file which is otherwise restricted. On	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploitation an attacker can completely compromise the confidentiality of the application. **CVE ID : CVE-2022-41212**		
URL Redirection to Untrusted Site ('Open Redirect')	08-Nov-2022	4.7	SAP NetWeaver ABAP Server and ABAP Platform allows an unauthenticated attacker to redirect users to a malicious site due to insufficient URL validation. This could lead to the user being tricked to disclose personal information. **CVE ID : CVE-2022-41215**	https://launchpad.support.sap.com/#/notes/3251202, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-221122/861
Affected Version(s): 789					
Improper Input Validation	08-Nov-2022	6.5	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to delete a file which is otherwise restricted. On successful exploitation an attacker can	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			completely compromise the integrity and availability of the application. **CVE ID : CVE-2022-41214**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	4.9	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to read a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the confidentiality of the application. **CVE ID : CVE-2022-41212**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/863
URL Redirection to Untrusted Site ('Open Redirect')	08-Nov-2022	4.7	SAP NetWeaver ABAP Server and ABAP Platform allows an unauthenticated attacker to redirect users to a malicious site due to insufficient URL validation. This could lead to the user being tricked	https://launchpad.support.sap.com/#/notes/3251202, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-221122/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to disclose personal information. **CVE ID : CVE-2022-41215**		
Affected Version(s): 804					
Improper Input Validation	08-Nov-2022	6.5	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to delete a file which is otherwise restricted. On successful exploitation an attacker can completely compromise the integrity and availability of the application. **CVE ID : CVE-2022-41214**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/865
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	4.9	Due to insufficient input validation, SAP NetWeaver Application Server ABAP and ABAP Platform allows an attacker with high level privileges to use a remote enabled function to read a file which is otherwise restricted. On successful	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3256571	A-SAP-NETW-221122/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation an attacker can completely compromise the confidentiality of the application. **CVE ID : CVE-2022-41212**		
Product: sql_anywhere					
Affected Version(s): 17.0					
N/A	08-Nov-2022	6.5	SAP SQL Anywhere - version 17.0, allows an authenticated attacker to prevent legitimate users from accessing a SQL Anywhere database server by crashing the server with some queries that use an ARRAY constructor. **CVE ID : CVE-2022-41259**	https://launchpad.support.sap.com/#/notes/3229987, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SQL_-221122/867
Vendor: Schneider-electric					
Product: ecostruxure_operator_terminal_expert					
Affected Version(s): * Up to (excluding) 3.3					
Improper Verification of Cryptographic Signature	04-Nov-2022	7.8	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code.	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41666**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-2022	7.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41667**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/869
Incorrect Type Conversion or Cast	04-Nov-2022	7.8	A CWE-704: Incorrect Project Conversion vulnerability exists that allows adversaries with local user privileges to load a project file from an adversary-controlled network	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			share which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41668**		
Improper Verification of Cryptographic Signature	04-Nov-2022	7.8	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load a malicious DLL which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41669**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/871
Improper Limitation of a Pathname to a Restricted Directory	04-Nov-2022	7.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load malicious DLL which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41670**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Nov-2022	7.8	A CWE-89: Improper Neutralization of Special Elements used in SQL Command ('SQL Injection') vulnerability exists that allows adversaries with local user privileges to craft a malicious SQL query and execute as part of project migration which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41671**		
Affected Version(s): 3.3					
Improper Verification of Cryptographic Signature	04-Nov-2022	7.8	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41666**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/874
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-2022	7.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code.	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41667**		
Incorrect Type Conversion or Cast	04-Nov-2022	7.8	A CWE-704: Incorrect Project Conversion vulnerability exists that allows adversaries with local user privileges to load a project file from an adversary-controlled network share which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41668**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/876
Improper Verification of Cryptographic Signature	04-Nov-2022	7.8	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load a malicious DLL	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41669**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-2022	7.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load malicious DLL which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41670**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-ECOS-221122/878
Improper Neutralization of Special Elements	04-Nov-2022	7.8	A CWE-89: Improper Neutralization of Special Elements used in SQL	https://www.se.com/ww/en/download/document/SE	A-SCH-ECOS-221122/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Command ('SQL Injection') vulnerability exists that allows adversaries with local user privileges to craft a malicious SQL query and execute as part of project migration which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41671**	VD-2022-284-01/	
Product: pro-face_blue					
Affected Version(s): * Up to (excluding) 3.3					
Improper Verification of Cryptographic Signature	04-Nov-2022	7.8	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41666**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-2022	7.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41667**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/881
Incorrect Type Conversion or Cast	04-Nov-2022	7.8	A CWE-704: Incorrect Project Conversion vulnerability exists that allows adversaries with local user privileges to load a project file from an adversary-controlled network share which could result in execution of malicious code. Affected Products: EcoStruxure	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41668**		
Improper Verification of Cryptographic Signature	04-Nov-2022	7.8	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load a malicious DLL which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41669**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/883
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-2022	7.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in the SGIUtility component that allows adversaries with local user	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to load malicious DLL which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41670**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Nov-2022	7.8	A CWE-89: Improper Neutralization of Special Elements used in SQL Command ('SQL Injection') vulnerability exists that allows adversaries with local user privileges to craft a malicious SQL query and execute as part of project migration which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41671**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/885
Affected Version(s): 3.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	04-Nov-2022	7.8	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41666**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/886
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-2022	7.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41667**		
Incorrect Type Conversion or Cast	04-Nov-2022	7.8	A CWE-704: Incorrect Project Conversion vulnerability exists that allows adversaries with local user privileges to load a project file from an adversary-controlled network share which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41668**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/888
Improper Verification of Cryptographic Signature	04-Nov-2022	7.8	A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load a malicious DLL which could result in execution of malicious code. Affected Products: EcoStruxure	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41669**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Nov-2022	7.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load malicious DLL which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41670**	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/890
Improper Neutralization of Special Elements used in an SQL Command	04-Nov-2022	7.8	A CWE-89: Improper Neutralization of Special Elements used in SQL Command ('SQL Injection') vulnerability exists that allows adversaries with	https://www.se.com/ww/en/download/document/SEVD-2022-284-01/	A-SCH-PRO--221122/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			local user privileges to craft a malicious SQL query and execute as part of project migration which could result in execution of malicious code. Affected Products: EcoStruxure Operator Terminal Expert(V3.3 Hotfix 1 or prior), Pro-face BLUE(V3.3 Hotfix1 or prior). **CVE ID : CVE-2022-41671**		
Vendor: searchwp					
Product: searchwp					
Affected Version(s): * Up to (including) 4.2.5					
Missing Authorization	08-Nov-2022	4.3	Nonce token leakage and missing authorization in SearchWP premium plugin <= 4.2.5 on WordPress leading to plugin settings change. **CVE ID : CVE-2022-40223**	https://searchwp.com/documentation/changelog/, https://patchstack.com/database/vulnerability/searchwp/wordpress-searchwp-premium-plugin-4-2-5-broken-authentication-vulnerability?_s_id=cve	A-SEA-SEAR-221122/892
Vendor: sedlex					
Product: traffic_manager					
Affected Version(s): * Up to (including) 1.4.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Broken Access Control vulnerability leading to Stored Cross-Site Scripting (XSS) in Traffic Manager plugin <= 1.4.5 on WordPress. **CVE ID : CVE-2022-42460**	https://patchstack.com/database/vulnerability/traffic-manager/wordpress-traffic-manager-plugin-1-4-5-broken-access-control-vulnerability-leading-to-stored-cross-site-scripting-xss?_s_id=cve, https://wordpress.org/plugins/traffic-manager/	A-SED-TRAF-221122/893
Vendor: shopwind					
Product: shopwind					
Affected Version(s): 3.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-2022	6.1	Shopwind v3.4.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in the component /common/library/Page.php. **CVE ID : CVE-2022-43321**	N/A	A-SHO-SHOP-221122/894
Vendor: Siemens					
Product: jt2go					
Affected Version(s): * Up to (excluding) 14.1.0.4					
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-JT2G-221122/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V13.3 (All versions >= V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application is vulnerable to fixed-length heap-based buffer while parsing specially crafted TIF files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-39136**		
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-JT2G-221122/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V14.1.0.4). The affected products contain an out of bounds write vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41660**		
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-JT2G-221122/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41661		
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41662**	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-JT2G-221122/898
Use After Free	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3),	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-JT2G-221122/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted CGM files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41663**		
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application contains a stack-based buffer overflow vulnerability that could be triggered while parsing	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-JT2G-221122/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted PDF files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2022-41664**		
Product: parasolid					
Affected Version(s): From (including) 34.0 Up to (excluding) 34.0.252					
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17854) **CVE ID : CVE-2022-43397**	https://cert-portal.siemens.com/productcert/pdf/ssa-853037.pdf	A-SIE-PARA-221122/901
Affected Version(s): From (including) 34.0.252 Up to (excluding) 34.0.254					
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions <	https://cert-portal.siemens.com/produc	A-SIE-PARA-221122/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V34.0.252), Parasolid V34.0 (All versions >= V34.0.252 < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V34.1 (All versions >= V34.1.242 < V34.1.244), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.0 (All versions >= V35.0.170 < V35.0.184). The affected application contains an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17745) **CVE ID : CVE-2022-39157**	tcert/pdf/ssa-853037.pdf	
Affected Version(s): From (including) 34.1 Up to (excluding) 34.1.242					
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242),	https://cert-portal.siemens.com/productcert/pdf/ssa-853037.pdf	A-SIE-PARA-221122/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parasolid V35.0 (All versions < V35.0.170). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17854) **CVE ID : CVE-2022-43397**		
Affected Version(s): From (including) 34.1.242 Up to (excluding) 34.1.244					
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.0 (All versions >= V34.0.252 < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V34.1 (All versions >= V34.1.242 < V34.1.244), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.0 (All versions >= V35.0.170 < V35.0.184). The affected application	https://cert-portal.siemens.com/productcert/pdf/ssa-853037.pdf	A-SIE-PARA-221122/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17745) **CVE ID : CVE-2022-39157**		
Affected Version(s): From (including) 35.0 Up to (excluding) 35.0.170					
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17854) **CVE ID : CVE-2022-43397**	https://cert-portal.siemens.com/productcert/pdf/ssa-853037.pdf	A-SIE-PARA-221122/905
Affected Version(s): From (including) 35.0.170 Up to (excluding) 35.0.184					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.0 (All versions >= V34.0.252 < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V34.1 (All versions >= V34.1.242 < V34.1.244), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.0 (All versions >= V35.0.170 < V35.0.184). The affected application contains an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17745) **CVE ID : CVE-2022-39157**	https://cert-portal.siemens.com/productcert/pdf/ssa-853037.pdf	A-SIE-PARA-221122/906
Product: qms_automotive					
Affected Version(s): *					
Cleartext Storage of Sensitive	08-Nov-2022	9.1	A vulnerability has been identified in QMS Automotive	https://cert-portal.siemens.com/produc	A-SIE-QMS_-221122/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			(All versions). User credentials are stored in plaintext in the database. This could allow an attacker to gain access to credentials and impersonate other users. **CVE ID : CVE-2022-43958**	tcert/pdf/ssa-587547.pdf	
Product: simatic_s7-1500_software_controller					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	A-SIE-SIMA-221122/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-plcsim_advanced					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	A-SIE-SIMA-221122/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_wincc_runtime					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	A-SIE-SIMA-221122/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: teamcenter_visualization					
Affected Version(s): * Up to (including) 13.3.0.7					
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V13.3 (All versions >= V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application is vulnerable to fixed-length heap-based buffer while parsing specially crafted TIF files. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2022-39136**		
Affected Version(s): From (including) 13.3.0 Up to (excluding) 13.3.0.7					
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds write vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41660**	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/912
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7),	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41661**		
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41662**		
Use After Free	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted CGM files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41663**	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/915
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4),	https://cert-portal.siemens.com/produc	A-SIE-TEAM-221122/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application contains a stack-based buffer overflow vulnerability that could be triggered while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2022-41664**	tcert/pdf/ssa-120378.pdf	
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0.0.3					
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V13.3 (All versions >= V13.3.0.7), Teamcenter Visualization V14.0	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application is vulnerable to fixed-length heap-based buffer while parsing specially crafted TIF files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-39136**		
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds write vulnerability when parsing a CGM file. An attacker can leverage this	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41660**		
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41661**	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/919
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7),	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41662**		
Use After Free	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected applications contain a use-after-free vulnerability that could be triggered while	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing specially crafted CGM files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41663**		
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application contains a stack-based buffer overflow vulnerability that could be triggered while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2022-41664**	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1.0.4					
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V13.3 (All versions >= V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application is vulnerable to fixed-length heap-based buffer while parsing specially crafted TIF files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-39136**	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/923
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7),	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds write vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41660**		
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41661**		
Out-of-bounds Read	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected products contain an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41662**	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/926
Use After Free	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted CGM files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2022-41663**		
Out-of-bounds Write	08-Nov-2022	7.8	A vulnerability has been identified in JT2Go (All versions < V14.1.0.4), Teamcenter Visualization V13.3 (All versions < V13.3.0.7), Teamcenter Visualization V14.0 (All versions < V14.0.0.3), Teamcenter Visualization V14.1 (All versions < V14.1.0.4). The affected application contains a stack-	https://cert-portal.siemens.com/productcert/pdf/ssa-120378.pdf	A-SIE-TEAM-221122/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based buffer overflow vulnerability that could be triggered while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2022-41664**		
Vendor: silabs					
Product: gecko_bootloader					
Affected Version(s): * Up to (including) 4.0.1					
Out-of-bounds Write	02-Nov-2022	9.1	Out-of-Bounds error in GBL parser in Silicon Labs Gecko Bootloader version 4.0.1 and earlier allows attacker to overwrite flash Sign key and OTA decryption key via malicious bootloader upgrade. **CVE ID : CVE-2022-24936**	https://community.silabs.com/sfc/servlet.shepherd/document/download/0698Y00000Gdop4QAB?operationContext=S1	A-SIL-GECK-221122/929
Vendor: simple_cashiering_system_project					
Product: simple_cashiering_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page	11-Nov-2022	6.1	A vulnerability, which was classified as problematic, has been found in Sourcecodester	N/A	A-SIM-SIMP-221122/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Simple Cashiering System. This issue affects some unknown processing of the component User Account Handler. The manipulation of the argument fullname leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-213455. **CVE ID : CVE-2022-3949**		
Vendor: simple_e-learning_system_project					
Product: simple_e-learning_system					
Affected Version(s): 1.0					
N/A	07-Nov-2022	7.5	An information disclosure vulnerability in the component vcs/downloadFiles.php?download=./search.php of Simple E-Learning System v1.0 allows attackers to read arbitrary files. **CVE ID : CVE-2022-43319**	N/A	A-SIM-SIMP-221122/931
Vendor: simple_video_embedder_project					
Product: simple_video_embedder					
Affected Version(s): * Up to (including) 2.2					
Improper Neutralization of	09-Nov-2022	5.4	Auth. (contributor+) Stored Cross-Site	https://patchstack.com/database/vulnerab	A-SIM-SIMP-221122/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability in James Lao's Simple Video Embedder plugin <= 2.2 on WordPress. **CVE ID : CVE-2022-44590**	ility/simple-video-embedder/wordpress-simple-video-embedder-plugin-2-2-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve, https://wordpress.org/plugins/simple-video-embedder/	
Vendor: slidervilla					
Product: testimonial_slider					
Affected Version(s): * Up to (including) 1.3.1					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability leading to Cross-Site Scripting (XSS) in David Anderson Testimonial Slider plugin <= 1.3.1 on WordPress. **CVE ID : CVE-2022-44741**	https://wordpress.org/plugins/testimonial-slider/, https://patchstack.com/database/vulnerability/testimonial-slider/wordpress-testimonial-slider-plugin-1-3-1-cross-site-request-forgery-csrf-vulnerability?_s_id=cve	A-SLI-TEST-221122/933
Vendor: Slims					
Product: senayan_library_management_system					
Affected Version(s): 9.4.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	7.2	Senayan Library Management System v9.4.2 was discovered to contain a SQL injection vulnerability via the collType parameter at loan_by_class.php. **CVE ID : CVE-2022-43362**	N/A	A-SLI-SENA-221122/934
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-2022	4.8	Senayan Library Management System v9.4.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the component pop_chart.php. **CVE ID : CVE-2022-43361**	N/A	A-SLI-SENA-221122/935
Vendor: snakeyaml_project					
Product: snakeyaml					
Affected Version(s): * Up to (excluding) 1.32					
Out-of-bounds Write	11-Nov-2022	6.5	Those using Snakeyaml to parse untrusted YAML files 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 stack overflow. This effect may support	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50355	A-SNA-SNAK-221122/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service attack. **CVE ID : CVE-2022-41854**		
Vendor: Snowflake					
Product: snowflake-connector-python					
Affected Version(s): -					
N/A	09-Nov-2022	7.5	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the snowflake-connector-python PyPI package, when an attacker is able to supply arbitrary input to the get_file_transfer_type method **CVE ID : CVE-2022-42965**	N/A	A-SNO-SNOW-221122/937
Vendor: soflyy					
Product: wp_all_import					
Affected Version(s): * Up to (excluding) 3.6.9					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Nov-2022	7.2	The Import any XML or CSV File to WordPress plugin before 3.6.9 is not validating the paths of files contained in uploaded zip archives, allowing highly privileged users, such as admins, to write arbitrary files to any part of the file system accessible by the web server	https://wpscan.com/vulnerability/11e73c23-ff5f-42e5-a4b0-0971652dcea1	A-SOF-WP_A-221122/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a path traversal vector. **CVE ID : CVE-2022-2711**		
Improper Control of Generation of Code ('Code Injection')	07-Nov-2022	7.2	The Import any XML or CSV File to WordPress plugin before 3.6.9 is not properly filtering which file extensions are allowed to be imported on the server, which could allow administrators in multi-site WordPress installations to upload arbitrary files **CVE ID : CVE-2022-3418**	https://wpscan.com/vulnerability/ccbb74f5-1b8f-4ea6-96bc-ddf62af7f94d	A-SOF-WP_A-221122/939
Vendor: Splunk					
Product: splunk					
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.12					
Improper Input Validation	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9 and 8.1.12, the way that the rex search command handles field names lets an attacker bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards . The vulnerability	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1103.html	A-SPL-SPLU-221122/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requires the attacker to phish the victim by tricking them into initiating a request within their browser. The attacker cannot exploit the vulnerability at will. **CVE ID : CVE-2022-43563**		
Improper Input Validation	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9 and 8.1.12, the way that the 'tstats command handles Javascript Object Notation (JSON) lets an attacker bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards . The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. **CVE ID : CVE-2022-43565**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1105.html	A-SPL-SPLU-221122/941
N/A	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9, 8.1.12,	https://research.splunk.com/application/	A-SPL-SPLU-221122/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 9.0.2, an authenticated user can run arbitrary operating system commands remotely through the use of specially crafted requests to the mobile alerts feature in the Splunk Secure Gateway app. **CVE ID : CVE-2022-43567**	baa41f09-df48-4375-8991-520beea161be/, https://www.splunk.com/en_us/product-security/announcements/svd-2022-1107.html	
Improper Control of Generation of Code ('Code Injection')	03-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can execute arbitrary code through the dashboard PDF generation component. **CVE ID : CVE-2022-43571**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1111.html, https://research.splunk.com/application/b06b41d7-9570-4985-8137-0784f582a1b3/	A-SPL-SPLU-221122/943
Improper Privilege Management	04-Nov-2022	8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run risky commands using a more privileged user's permissions to bypass SPL safeguards for risky commands https://docs.splunk.com/Documentatio	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1106.html, https://research.splunk.com/application/b6d77c6c-f011-4b03-8650-	A-SPL-SPLU-221122/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n/SplunkCloud/latest/Security/SPLsafeguards in the Analytics Workspace. The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The attacker cannot exploit the vulnerability at will. **CVE ID : CVE-2022-43566**	8f10edb7c4a8/	
Uncontrolled Resource Consumption	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a remote user who can create search macros and schedule search reports can cause a denial of service through the use of specially crafted search macros. **CVE ID : CVE-2022-43564**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1104.html	A-SPL-SPLU-221122/945
Improper Restriction of XML External Entity Reference	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, an authenticated user can perform an extensible markup language (XML) external entity (XXE) injection via	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1110.html	A-SPL-SPLU-221122/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a custom View. The XXE injection causes Splunk Web to embed incorrect documents into an error. **CVE ID : CVE-2022-43570**		
Improper Control of Generation of Code ('Code Injection')	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, sending a malformed file through the Splunk-to-Splunk (S2S) or HTTP Event Collector (HEC) protocols to an indexer results in a blockage or denial-of-service preventing further indexing. **CVE ID : CVE-2022-43572**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1111.html	A-SPL-SPLU-221122/947
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	6.1	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a View allows for a Reflected Cross Site Scripting via JavaScript Object Notation (JSON) in a query parameter when output_mode=radio . **CVE ID : CVE-2022-43568**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1108.html, https://research.splunk.com/application/d532d105-c63f-4049-a8c4-e249127ca425/	A-SPL-SPLU-221122/948
Improper Neutralizat	04-Nov-2022	5.4	In Splunk Enterprise versions	https://www.splunk.com/e	A-SPL-SPLU-221122/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements in Output Used by a Downstream Component ('Injection')			below 8.1.12, 8.2.9, and 9.0.2, Splunk Enterprise fails to properly validate and escape the Host header, which could let a remote authenticated user conduct various attacks against the system, including cross-site scripting and cache poisoning. **CVE ID : CVE-2022-43562**	n_us/product-security/announcements/svd-2022-1102.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	5.4	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, an authenticated user can inject and store arbitrary scripts that can lead to persistent cross-site scripting (XSS) in the object name of a Data Model. **CVE ID : CVE-2022-43569**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1109.html, https://research.splunk.com/application/062bff76-5f9c-496e-a386-cb1adcf69871/	A-SPL-SPLU-221122/950
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	4.8	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a remote user that holds the "power" Splunk role can store arbitrary scripts that can lead to persistent cross-site scripting (XSS). The vulnerability	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1101.html, https://research.splunk.com/application/a974d1ee-ddca-4837-	A-SPL-SPLU-221122/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects instances with Splunk Web enabled. **CVE ID : CVE-2022-43561**	b6ad-d55a8a239c20/	
Affected Version(s): From (including) 8.2.0 Up to (excluding) 8.2.9					
Improper Input Validation	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9 and 8.1.12, the way that the rex search command handles field names lets an attacker bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards . The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The attacker cannot exploit the vulnerability at will. **CVE ID : CVE-2022-43563**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1103.html	A-SPL-SPLU-221122/952
Improper Input Validation	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9 and 8.1.12, the way that the 'tstats command handles Javascript Object	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1105.html	A-SPL-SPLU-221122/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Notation (JSON) lets an attacker bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards . The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. **CVE ID : CVE-2022-43565**		
N/A	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run arbitrary operating system commands remotely through the use of specially crafted requests to the mobile alerts feature in the Splunk Secure Gateway app. **CVE ID : CVE-2022-43567**	https://research.splunk.com/application/baa41f09-df48-4375-8991-520beea161be/, https://www.splunk.com/en_us/product-security/announcements/svd-2022-1107.html	A-SPL-SPLU-221122/954
Improper Control of Generation of Code	03-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can execute	https://www.splunk.com/en_us/product-security/announcements/svd-2022-	A-SPL-SPLU-221122/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			arbitrary code through the dashboard PDF generation component. **CVE ID : CVE-2022-43571**	1111.html, https://research.splunk.com/application/b06b41d7-9570-4985-8137-0784f582a1b3/	
Improper Privilege Management	04-Nov-2022	8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run risky commands using a more privileged user's permissions to bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards in the Analytics Workspace. The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The attacker cannot exploit the vulnerability at will. **CVE ID : CVE-2022-43566**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1106.html, https://research.splunk.com/application/b6d77c6c-f011-4b03-8650-8f10edb7c4a8/	A-SPL-SPLU-221122/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a remote user who can create search macros and schedule search reports can cause a denial of service through the use of specially crafted search macros. **CVE ID : CVE-2022-43564**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1104.html	A-SPL-SPLU-221122/957
Improper Restriction of XML External Entity Reference	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, an authenticated user can perform an extensible markup language (XML) external entity (XXE) injection via a custom View. The XXE injection causes Splunk Web to embed incorrect documents into an error. **CVE ID : CVE-2022-43570**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1110.html	A-SPL-SPLU-221122/958
Improper Control of Generation of Code ('Code Injection')	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, sending a malformed file through the Splunk-to-Splunk (S2S) or HTTP Event Collector (HEC) protocols to an indexer results in a	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1111.html	A-SPL-SPLU-221122/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			blockage or denial-of-service preventing further indexing. **CVE ID : CVE-2022-43572**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	6.1	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a View allows for a Reflected Cross Site Scripting via JavaScript Object Notation (JSON) in a query parameter when output_mode=radio. **CVE ID : CVE-2022-43568**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1108.html, https://research.splunk.com/application/d532d105-c63f-4049-a8c4-e249127ca425/	A-SPL-SPLU-221122/960
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Nov-2022	5.4	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, Splunk Enterprise fails to properly validate and escape the Host header, which could let a remote authenticated user conduct various attacks against the system, including cross-site scripting and cache poisoning. **CVE ID : CVE-2022-43562**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1102.html	A-SPL-SPLU-221122/961
Improper Neutralization of	04-Nov-2022	5.4	In Splunk Enterprise versions below 8.1.12, 8.2.9,	https://www.splunk.com/en_us/product-	A-SPL-SPLU-221122/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			and 9.0.2, an authenticated user can inject and store arbitrary scripts that can lead to persistent cross-site scripting (XSS) in the object name of a Data Model. **CVE ID : CVE-2022-43569**	security/announcements/svd-2022-1109.html, https://research.splunk.com/application/062bff76-5f9c-496e-a386-cb1adcf69871/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	4.8	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a remote user that holds the "power" Splunk role can store arbitrary scripts that can lead to persistent cross-site scripting (XSS). The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2022-43561**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1101.html, https://research.splunk.com/application/a974d1ee-ddca-4837-b6ad-d55a8a239c20/	A-SPL-SPLU-221122/963
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.2					
N/A	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run arbitrary operating system commands remotely through the use of specially crafted requests to the mobile alerts feature in the	https://research.splunk.com/application/baa41f09-df48-4375-8991-520beea161be/, https://www.splunk.com/en_us/product-security/announcements/sv	A-SPL-SPLU-221122/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Splunk Secure Gateway app. **CVE ID : CVE-2022-43567**	d-2022-1107.html	
Improper Control of Generation of Code ('Code Injection')	03-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can execute arbitrary code through the dashboard PDF generation component. **CVE ID : CVE-2022-43571**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1111.html, https://research.splunk.com/application/b06b41d7-9570-4985-8137-0784f582a1b3/	A-SPL-SPLU-221122/965
Improper Privilege Management	04-Nov-2022	8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run risky commands using a more privileged user's permissions to bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards in the Analytics Workspace. The vulnerability requires the attacker to phish the victim by tricking them into	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1106.html, https://research.splunk.com/application/b6d77c6c-f011-4b03-8650-8f10edb7c4a8/	A-SPL-SPLU-221122/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiating a request within their browser. The attacker cannot exploit the vulnerability at will. **CVE ID : CVE-2022-43566**		
Improper Restriction of XML External Entity Reference	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, an authenticated user can perform an extensible markup language (XML) external entity (XXE) injection via a custom View. The XXE injection causes Splunk Web to embed incorrect documents into an error. **CVE ID : CVE-2022-43570**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1110.html	A-SPL-SPLU-221122/967
Improper Control of Generation of Code ('Code Injection')	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, sending a malformed file through the Splunk-to-Splunk (S2S) or HTTP Event Collector (HEC) protocols to an indexer results in a blockage or denial-of-service preventing further indexing.	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1111.html	A-SPL-SPLU-221122/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43572		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	6.1	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a View allows for a Reflected Cross Site Scripting via JavaScript Object Notation (JSON) in a query parameter when output_mode=radio. **CVE ID : CVE-2022-43568**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1108.html, https://research.splunk.com/application/d532d105-c63f-4049-a8c4-e249127ca425/	A-SPL-SPLU-221122/969
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Nov-2022	5.4	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, Splunk Enterprise fails to properly validate and escape the Host header, which could let a remote authenticated user conduct various attacks against the system, including cross-site scripting and cache poisoning. **CVE ID : CVE-2022-43562**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1102.html	A-SPL-SPLU-221122/970
Improper Neutralization of Input During Web Page Generation	04-Nov-2022	5.4	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, an authenticated user can inject and store arbitrary scripts	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1109.html,	A-SPL-SPLU-221122/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			that can lead to persistent cross-site scripting (XSS) in the object name of a Data Model. **CVE ID : CVE-2022-43569**	https://research.splunk.com/application/062bff76-5f9c-496e-a386-cb1adcf69871/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	4.8	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a remote user that holds the "power" Splunk role can store arbitrary scripts that can lead to persistent cross-site scripting (XSS). The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2022-43561**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1101.html, https://research.splunk.com/application/a974d1ee-ddca-4837-b6ad-d55a8a239c20/	A-SPL-SPLU-221122/972
Product: splunk_cloud_platform					
Affected Version(s): * Up to (excluding) 9.0.2203					
Improper Input Validation	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9 and 8.1.12, the way that the rex search command handles field names lets an attacker bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards . The	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1103.html	A-SPL-SPLU-221122/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The attacker cannot exploit the vulnerability at will. **CVE ID : CVE-2022-43563**		
Improper Input Validation	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9 and 8.1.12, the way that the 'tstats command handles Javascript Object Notation (JSON) lets an attacker bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards . The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. **CVE ID : CVE-2022-43565**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1105.html	A-SPL-SPLU-221122/974
Affected Version(s): * Up to (excluding) 9.0.2205					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run arbitrary operating system commands remotely through the use of specially crafted requests to the mobile alerts feature in the Splunk Secure Gateway app. **CVE ID : CVE-2022-43567**	https://research.splunk.com/application/baa41f09-df48-4375-8991-520beea161be/, https://www.splunk.com/en_us/product-security/announcements/svd-2022-1107.html	A-SPL-SPLU-221122/975
Uncontrolled Resource Consumption	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a remote user who can create search macros and schedule search reports can cause a denial of service through the use of specially crafted search macros. **CVE ID : CVE-2022-43564**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1104.html	A-SPL-SPLU-221122/976
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	6.1	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a View allows for a Reflected Cross Site Scripting via JavaScript Object Notation (JSON) in a query parameter when	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1108.html, https://research.splunk.com/application/d532d105-c63f-4049-	A-SPL-SPLU-221122/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			output_mode=radio . **CVE ID : CVE-2022-43568**	a8c4-e249127ca425/	
Affected Version(s): * Up to (excluding) 9.0.2208					
Improper Privilege Management	04-Nov-2022	8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can run risky commands using a more privileged user's permissions to bypass SPL safeguards for risky commands https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/SPLsafeguards in the Analytics Workspace. The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The attacker cannot exploit the vulnerability at will. **CVE ID : CVE-2022-43566**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1106.html, https://research.splunk.com/application/b6d77c6c-f011-4b03-8650-8f10edb7c4a8/	A-SPL-SPLU-221122/978
Improper Neutralization of Special	04-Nov-2022	5.4	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, Splunk	https://www.splunk.com/en_us/product-security/anno	A-SPL-SPLU-221122/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			Enterprise fails to properly validate and escape the Host header, which could let a remote authenticated user conduct various attacks against the system, including cross-site scripting and cache poisoning. **CVE ID : CVE-2022-43562**	uncements/svd-2022-1102.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	4.8	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, a remote user that holds the "power" Splunk role can store arbitrary scripts that can lead to persistent cross-site scripting (XSS). The vulnerability affects instances with Splunk Web enabled. **CVE ID : CVE-2022-43561**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1101.html, https://research.splunk.com/application/a974d1ee-ddca-4837-b6ad-d55a8a239c20/	A-SPL-SPLU-221122/980
Affected Version(s): * Up to (excluding) 9.0.2209					
Improper Control of Generation of Code ('Code Injection')	03-Nov-2022	8.8	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, an authenticated user can execute arbitrary code through the dashboard PDF	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1111.html, https://research.splunk.com/application/	A-SPL-SPLU-221122/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generation component. **CVE ID : CVE-2022-43571**	b06b41d7-9570-4985-8137-0784f582a1b3/	
Improper Restriction of XML External Entity Reference	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.1.12, 8.2.9, and 9.0.2, an authenticated user can perform an extensible markup language (XML) external entity (XXE) injection via a custom View. The XXE injection causes Splunk Web to embed incorrect documents into an error. **CVE ID : CVE-2022-43570**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1110.html	A-SPL-SPLU-221122/982
Improper Control of Generation of Code ('Code Injection')	04-Nov-2022	6.5	In Splunk Enterprise versions below 8.2.9, 8.1.12, and 9.0.2, sending a malformed file through the Splunk-to-Splunk (S2S) or HTTP Event Collector (HEC) protocols to an indexer results in a blockage or denial-of-service preventing further indexing. **CVE ID : CVE-2022-43572**	https://www.splunk.com/en_us/product-security/announcements/svd-2022-1111.html	A-SPL-SPLU-221122/983
Improper Neutralizat	04-Nov-2022	5.4	In Splunk Enterprise versions	https://www.splunk.com/e	A-SPL-SPLU-221122/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			below 8.1.12, 8.2.9, and 9.0.2, an authenticated user can inject and store arbitrary scripts that can lead to persistent cross-site scripting (XSS) in the object name of a Data Model. **CVE ID : CVE-2022-43569**	n_us/product-security/announcements/svd-2022-1109.html, https://research.splunk.com/application/062bff76-5f9c-496e-a386-cb1adcf69871/	
Vendor: stiltsoft					
Product: handy_macros_for_confluence					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Nov-2022	5.4	The Handy Tip macro in Stiltsoft Handy Macros for Confluence Server/Data Center 3.x before 3.5.5 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2022-44724**	https://stiltsoft.atlassian.net/browse/VD-3	A-STI-HAND-221122/985
Vendor: struktur					
Product: libde265					
Affected Version(s): 1.0.8					
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via ff_hevc_put_hevc_epel_pixels_8_sse in sse-motion.cc. This	N/A	A-STR-LIBD-221122/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43235**		
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a stack-buffer-overflow vulnerability via put_qpel_fallback<unsigned short> in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43236**	N/A	A-STR-LIBD-221122/987
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a stack-buffer-overflow vulnerability via void put_epel_hv_fallback<unsigned short> in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43237**	N/A	A-STR-LIBD-221122/988
N/A	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain an	N/A	A-STR-LIBD-221122/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unknown crash via ff_hevc_put_hevc_qpel_h_3_v_3_sse in sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43238**		
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via mc_chroma<unsigned short> in motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43239**	N/A	A-STR-LIBD-221122/990
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via ff_hevc_put_hevc_qpel_h_2_v_1_sse in sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43240**	N/A	A-STR-LIBD-221122/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain an unknown crash via ff_hevc_put_hevc_qpel_v_3_8_sse in sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43241**	N/A	A-STR-LIBD-221122/992
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via mc_luma<unsigned char> in motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43242**	N/A	A-STR-LIBD-221122/993
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via ff_hevc_put_weighted_pred_avg_8_sse in sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file.	N/A	A-STR-LIBD-221122/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43243		
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_qpel_fallback<unsigned short> in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43244**	N/A	A-STR-LIBD-221122/995
N/A	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a segmentation violation via apply_sao_internal<unsigned short> in sao.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43245**	N/A	A-STR-LIBD-221122/996
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_weighted_pred_avg_16_fallback in fallback-motion.cc. This vulnerability allows attackers to	N/A	A-STR-LIBD-221122/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43248**		
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_epel_hv_fallback<unsigned short> in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43249**	N/A	A-STR-LIBD-221122/998
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_qpel_0_0_fallback_16 in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43250**	N/A	A-STR-LIBD-221122/999
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_epel_16_fallbac	N/A	A-STR-LIBD-221122/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			k in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43252**		
Out-of-bounds Write	02-Nov-2022	6.5	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via put_unweighted_pred_16_fallback in fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted video file. **CVE ID : CVE-2022-43253**	N/A	A-STR-LIBD-221122/1001
Vendor: sudo_project					
Product: sudo					
Affected Version(s): From (including) 1.8.0 Up to (including) 1.9.12					
Out-of-bounds Read	02-Nov-2022	7.1	Sudo 1.8.0 through 1.9.12, with the crypt() password backend, contains a plugins/sudoers/auth/passwd.c array-out-of-bounds error that can result in a heap-based buffer over-read. This can be triggered by arbitrary local users with access to Sudo by entering a	https://github.com/sudo-project/sudo/commit/bd209b9f16fcd1270c13db27ae3329c677d48050, https://www.sudo.ws/security/advisories/	A-SUD-SUDO-221122/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password of seven characters or fewer. The impact could vary depending on the system libraries, compiler, and processor architecture. **CVE ID : CVE-2022-43995**		
Vendor: Suse					
Product: manager_server					
Affected Version(s): From (including) 4.2 Up to (excluding) 4.2.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to embed Javascript code via /rhn/audit/scap/Search.do This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-	https://bugzilla.suse.com/show_bug.cgi?id=1204741	A-SUS-MANA-221122/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10. **CVE ID : CVE-2022-43754**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Nov-2022	4.3	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to read files available to the user running the process, typically tomcat. This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-	https://bugzilla.suse.com/show_bug.cgi?id=1204543	A-SUS-MANA-221122/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10. **CVE ID : CVE-2022-31255**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Nov-2022	4.3	A Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to read files available to the user running the process, typically tomcat. This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2,	https://bugzilla.suse.com/show_bug.cgi?id=1204716	A-SUS-MANA-221122/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 4.2.10. **CVE ID : CVE-2022-43753**		
Affected Version(s): From (including) 4.3 Up to (excluding) 4.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to embed Javascript code via /rhn/audit/scap/Search.do This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2,	https://bugzilla.suse.com/show_bug.cgi?id=1204741	A-SUS-MANA-221122/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43754		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Nov-2022	4.3	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to read files available to the user running the process, typically tomcat. This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-	https://bugzilla.suse.com/show_bug.cgi?id=1204543	A-SUS-MANA-221122/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10. **CVE ID : CVE-2022-31255**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Nov-2022	4.3	A Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to read files available to the user running the process, typically tomcat. This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4,	https://bugzilla.suse.com/show_bug.cgi?id=1204716	A-SUS-MANA-221122/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10. **CVE ID : CVE-2022-43753**		
Vendor: Symantec					
Product: endpoint_detection_and_response					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.7.0					
N/A	08-Nov-2022	9.8	Symantec Endpoint Detection and Response (SEDR) Appliance, prior to 4.7.0, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user. **CVE ID : CVE-2022-37015**	https://support.broadcom.com/external/content/SecurityAdvisories/0/21005	A-SYM-ENDP-221122/1009
Vendor: sysstat_project					
Product: sysstat					
Affected Version(s): From (including) 9.1.6 Up to (excluding) 12.7.1					
Incorrect Calculation of Buffer Size	08-Nov-2022	9.8	sysstat is a set of system performance tools for the Linux operating system. On 32 bit systems, in versions 9.1.16 and newer but prior to 12.7.1, allocate_structures contains a size_t overflow in sa_common.c. The allocate_structures function insufficiently	https://github.com/sysstat/sysstat/security/advisories/GHSA-q8r6-g56f-9w7x	A-SYS-SYSS-221122/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checks bounds before arithmetic multiplication, allowing for an overflow in the size allocated for the buffer representing system activities. This issue may lead to Remote Code Execution (RCE). This issue has been patched in version 12.7.1. **CVE ID : CVE-2022-39377**		
Vendor: systemd_project					
Product: systemd					
Affected Version(s): * Up to (including) 251					
Off-by-one Error	08-Nov-2022	5.5	An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service. **CVE ID : CVE-2022-3821**	https://github.com/systemd/systemd/commit/9102c625a673a3246d7e73d8737f3494446bad4e, https://github.com/systemd/systemd/pull/23933	A-SYS-SYST-221122/1011
Vendor: tagdiv_composer_project					
Product: tagdiv_composer					
Affected Version(s): * Up to (excluding) 3.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	14-Nov-2022	9.8	The tagDiv Composer WordPress plugin before 3.5, required by the Newspaper WordPress theme before 12.1 and Newsmag WordPress theme before 5.2.2, does not properly implement the Facebook login feature, allowing unauthenticated attackers to login as any user by just knowing their email address **CVE ID : CVE-2022-3477**	https://wpscan.com/vulnerability/993a95d2-6fce-48de-ae17-06ce2db829ef	A-TAG-TAGD-221122/1012
Vendor: tauri					
Product: tauri					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.0.7					
Use of Incorrectly-Resolved Name or Reference	10-Nov-2022	4.7	Tauri is a framework for building binaries for all major desktop platforms. In versions prior to 1.0.7 and 1.1.2, Tauri is vulnerable to an Incorrectly-Resolved Name. Due to incorrect escaping of special characters in paths selected via the file dialog and drag and drop functionality, it is possible to partially bypass the	https://github.com/tauri-apps/tauri/security/advisories/GHSA-q9wv-22m9-vhqh	A-TAU-TAUR-221122/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`fs` scope definition. It is not possible to traverse into arbitrary paths, as the issue is limited to neighboring files and sub folders of already allowed paths. The impact differs on Windows, MacOS and Linux due to different specifications of valid path characters. This bypass depends on the file picker dialog or dragged files, as user selected paths are automatically added to the allow list at runtime. A successful bypass requires the user to select a pre-existing malicious file or directory during the file picker dialog and an adversary controlled logic to access these files. The issue has been patched in versions 1.0.7, 1.1.2 and 1.2.0. As a workaround, disable the dialog and fileDropEnabled		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component inside the tauri.conf.json. **CVE ID : CVE-2022-41874**		
Affected Version(s): From (including) 1.1.0 Up to (excluding) 1.1.2					
Use of Incorrectly-Resolved Name or Reference	10-Nov-2022	4.7	Tauri is a framework for building binaries for all major desktop platforms. In versions prior to 1.0.7 and 1.1.2, Tauri is vulnerable to an Incorrectly-Resolved Name. Due to incorrect escaping of special characters in paths selected via the file dialog and drag and drop functionality, it is possible to partially bypass the `fs` scope definition. It is not possible to traverse into arbitrary paths, as the issue is limited to neighboring files and sub folders of already allowed paths. The impact differs on Windows, MacOS and Linux due to different specifications of valid path characters. This bypass depends on the file picker dialog or dragged	https://github.com/tauri-apps/tauri/security/advisories/GHSA-q9wv-22m9-vhqh	A-TAU-TAUR-221122/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files, as user selected paths are automatically added to the allow list at runtime. A successful bypass requires the user to select a pre-existing malicious file or directory during the file picker dialog and an adversary controlled logic to access these files. The issue has been patched in versions 1.0.7, 1.1.2 and 1.2.0. As a workaround, disable the dialog and fileDropEnabled component inside the tauri.conf.json. **CVE ID : CVE-2022-41874**		
Vendor: themepoints					
Product: testimonials					
Affected Version(s): * Up to (excluding) 2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	4.8	The Testimonials WordPress plugin before 2.7, super-testimonial-pro WordPress plugin before 1.0.8 do not sanitize and escape its settings, allowing high privilege users such as admin to perform cross-Site	https://wpscan.com/vulnerability/ab3b0052-1a74-4ba3-b6d2-78cfe56029db	A-THE-TEST-221122/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-3539**		
Product: testimonials_pro					
Affected Version(s): * Up to (excluding) 1.0.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	4.8	The Testimonials WordPress plugin before 2.7, super-testimonial-pro WordPress plugin before 1.0.8 do not sanitize 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-2022-3539**	https://wpscan.com/vulnerability/ab3b0052-1a74-4ba3-b6d2-78cfe56029db	A-THE-TEST-221122/1016
Vendor: tim_campus_confession_wall_project					
Product: tim_campus_confession_wall					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Nov-2022	9.8	A vulnerability has been found in Tim Campus Confession Wall and classified as critical. Affected by this vulnerability is an unknown functionality of the file share.php. The	N/A	A-TIM-TIM_-221122/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument post_id leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-212611. **CVE ID : CVE-2022-3789**		
Vendor: train_scheduler_app_project					
Product: train_scheduler_app					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-2022	6.1	A cross-site scripting (XSS) vulnerability in /admin/add-fee.php of Train Scheduler App v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cmddept parameter. **CVE ID : CVE-2022-43079**	N/A	A-TRA-TRAI-221122/1018
Vendor: trellix					
Product: intrusion_prevention_system_manager					
Affected Version(s): * Up to (excluding) 10.1					
Improper Restriction of XML External	04-Nov-2022	7.2	XML External Entity (XXE) vulnerability in Trellix IPS Manager prior to 10.1 M8 allows a remote	https://kcm.trellix.com/corporate/index?page=content&id=SB10388	A-TRE-INTR-221122/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity Reference			authenticated administrator to perform XXE attack in the administrator interface part of the interface, which allows a saved XML configuration file to be imported. **CVE ID : CVE-2022-3340**		
Affected Version(s): 10.1					
Improper Restriction of XML External Entity Reference	04-Nov-2022	7.2	XML External Entity (XXE) vulnerability in Trellix IPS Manager prior to 10.1 M8 allows a remote authenticated administrator to perform XXE attack in the administrator interface part of the interface, which allows a saved XML configuration file to be imported. **CVE ID : CVE-2022-3340**	https://kcm.trellix.com/corporate/index?page=content&id=SB10388	A-TRE-INTR-221122/1020
Vendor: Trihedral					
Product: vtscada					
Affected Version(s): * Up to (including) 12.0.38					
Improper Input Validation	02-Nov-2022	7.5	An Improper Input Validation vulnerability exists in Trihedral VTScada version 12.0.38 and prior. A specifically	https://www.cisa.gov/uscert/ics/advisories/icsa-22-300-04	A-TRI-VTSC-221122/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malformed HTTP request could cause the affected VTScada to crash. Both local area network (LAN)-only and internet facing systems are affected. **CVE ID : CVE-2022-3181**		
Vendor: tuxera					
Product: ntfs-3g					
Affected Version(s): * Up to (excluding) 2022.10.3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Nov-2022	7.8	A buffer overflow was discovered in NTFS-3G before 2022.10.3. Crafted metadata in an NTFS image can cause code execution. A local attacker can exploit this if the ntfs-3g binary is setuid root. A physically proximate attacker can exploit this if NTFS-3G software is configured to execute upon attachment of an external storage device. **CVE ID : CVE-2022-40284**	N/A	A-TUX-NTFS-221122/1022
Vendor: upspowercom					
Product: upsmon_pro					
Affected Version(s): 2.57					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	10-Nov-2022	9.8	UPSMON Pro login function has insufficient authentication. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and get administrator privilege to access, control system or disrupt service. **CVE ID : CVE-2022-38119**	N/A	A-UPS-UPSM-221122/1023
Cleartext Transmission of Sensitive Information	10-Nov-2022	7.5	UPSMON PRO transmits sensitive data in cleartext over HTTP protocol. An unauthenticated remote attacker can exploit this vulnerability to access sensitive data. **CVE ID : CVE-2022-38122**	N/A	A-UPS-UPSM-221122/1024
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Nov-2022	6.5	UPSMON PRO's has a path traversal vulnerability. A remote attacker with general user privilege can exploit this vulnerability to bypass authentication and access arbitrary system files.	N/A	A-UPS-UPSM-221122/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38120		
Insufficiently Protected Credentials	10-Nov-2022	6.5	UPSMON PRO configuration file stores user password in plaintext under public user directory. A remote attacker with general user privilege can access all users‘ and administrators' account names and passwords via this unprotected configuration file. **CVE ID : CVE-2022-38121**	N/A	A-UPS-UPSM-221122/1026
Vendor: uyuni-project					
Product: uyuni					
Affected Version(s): * Up to (excluding) 2022.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to embed Javascript	https://bugzilla.suse.com/show_bug.cgi?id=1204741	A-UYU-UYUN-221122/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code via /rhn/audit/scap/Search.do This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10. **CVE ID : CVE-2022-43754**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Nov-2022	4.3	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to read files available to the user running the process, typically tomcat. This issue affects:	https://bugzilla.suse.com/show_bug.cgi?id=1204543	A-UYU-UYUN-221122/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10. **CVE ID : CVE-2022-31255**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Nov-2022	4.3	A Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to read files available to the user running the process, typically tomcat. This issue affects: SUSE Linux Enterprise Module for SUSE Manager	https://bugzilla.suse.com/show_bug.cgi?id=1204716	A-UYU-UYUN-221122/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10. **CVE ID : CVE-2022-43753**		
Vendor: varnish-software					
Product: varnish_cache					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.11					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**		
Product: varnish_cache_plus					
Affected Version(s): 6.0.0					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1031
Affected Version(s): 6.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1032
Affected Version(s): 6.0.10					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**		
Affected Version(s): 6.0.2					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**		
Affected Version(s): 6.0.3					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1035
Affected Version(s): 6.0.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1036
Affected Version(s): 6.0.5					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**		
Affected Version(s): 6.0.6					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**		
Affected Version(s): 6.0.7					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1039
Affected Version(s): 6.0.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1040
Affected Version(s): 6.0.9					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**		
Vendor: varnish_cache_project					
Product: varnish_cache					
Affected Version(s): 7.2.0					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	09-Nov-2022	7.5	An issue was discovered in Varnish Cache 7.x before 7.1.2 and 7.2.x before 7.2.1. A request smuggling attack can be performed on Varnish Cache servers by requesting that certain headers are made hop-by-hop, preventing the Varnish Cache servers from forwarding critical headers to the backend.	https://varnish-cache.org/security/VSV00010.html	A-VAR-VARN-221122/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45059		
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1043
Affected Version(s): From (including) 5.0.0 Up to (excluding) 6.0.11					
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/sec	A-VAR-VARN-221122/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**	urity/VSV00011.html	
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.1.2					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	09-Nov-2022	7.5	An issue was discovered in Varnish Cache 7.x before 7.1.2 and 7.2.x before 7.2.1. A request smuggling attack can be performed on Varnish Cache servers by requesting that certain headers are made hop-by-hop, preventing the Varnish Cache servers from forwarding critical headers to the backend.	https://varnish-cache.org/security/VSV00010.html	A-VAR-VARN-221122/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45059		
N/A	09-Nov-2022	7.5	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected. **CVE ID : CVE-2022-45060**	https://docs.varnish-software.com/security/VSV00011, https://varnish-cache.org/security/VSV00011.html	A-VAR-VARN-221122/1046
Vendor: vehicle_booking_system_project					
Product: vehicle_booking_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	01-Nov-2022	7.2	An arbitrary file upload vulnerability in admin-add-vehicle.php of Vehicle Booking	N/A	A-VEH-VEHI-221122/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-43083**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-2022	4.8	A cross-site scripting (XSS) vulnerability in admin-add-vehicle.php of Vehicle Booking System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the v_name parameter. **CVE ID : CVE-2022-43084**	N/A	A-VEH-VEHI-221122/1048
Vendor: Vmware					
Product: bosh_editor					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.40.0					
Improper Control of Generation of Code ('Code Injection')	04-Nov-2022	9.8	Spring Tools 4 for Eclipse version 4.16.0 and below as well as VSCode extensions such as Spring Boot Tools, Concourse CI Pipeline Editor, Bosh Editor and Cloudfoundry Manifest YML Support version 1.39.0 and below all use Snakeyaml library for YAML editing support. This library allows for some special	https://tanzu.vmware.com/security/cve-2022-31691	A-VMW-BOSH-221122/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syntax in the YAML that under certain circumstances allows for potentially harmful remote code execution by the attacker. **CVE ID : CVE-2022-31691**		
Product: cloudfoundry_manifest_yml_support					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.40.0					
Improper Control of Generation of Code ('Code Injection')	04-Nov-2022	9.8	Spring Tools 4 for Eclipse version 4.16.0 and below as well as VSCode extensions such as Spring Boot Tools, Concourse CI Pipeline Editor, Bosh Editor and Cloudfoundry Manifest YML Support version 1.39.0 and below all use Snakeyaml library for YAML editing support. This library allows for some special syntax in the YAML that under certain circumstances allows for potentially harmful remote code execution by the attacker. **CVE ID : CVE-2022-31691**	https://tanzu.vmware.com/security/cve-2022-31691	A-VMW-CLOU-221122/1050
Product: concourse_ci_pipeline_editor					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.40.0					
Improper Control of Generation of Code ('Code Injection')	04-Nov-2022	9.8	Spring Tools 4 for Eclipse version 4.16.0 and below as well as VSCode extensions such as Spring Boot Tools, Concourse CI Pipeline Editor, Bosh Editor and Cloudfoundry Manifest YML Support version 1.39.0 and below all use Snakeyaml library for YAML editing support. This library allows for some special syntax in the YAML that under certain circumstances allows for potentially harmful remote code execution by the attacker. **CVE ID : CVE-2022-31691**	https://tanzu.vmware.com/security/cve-2022-31691	A-VMW-CONC-221122/1051
Product: hyperic_agent					
Affected Version(s): 5.8.6					
Deserialization of Untrusted Data	12-Nov-2022	9.9	** UNSUPPORTED WHEN ASSIGNED ** A remote insecure deserialization vulnerability exixsts in VMWare Hyperic Agent 5.8.6. Exploitation of this vulnerability enables a malicious	N/A	A-VMW-HYPE-221122/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to run arbitrary code or malware within a Hyperic Agent instance and its host operating system with the privileges of the Hyperic Agent process (often SYSTEM on Windows platforms). NOTE: prior exploitation of CVE-2022-38650 results in the disclosure of the authentication material required to exploit this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2022-38652**		
Product: hyperic_server					
Affected Version(s): 5.8.6					
N/A	12-Nov-2022	9.8	** UNSUPPORTED WHEN ASSIGNED ** A security filter misconfiguration exists in VMware Hyperic Server 5.8.6. Exploitation of this vulnerability enables a malicious party to bypass some authentication	N/A	A-VMW-HYPE-221122/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requirements when issuing requests to Hyperic Server. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2022-38651**		
Deserialization of Untrusted Data	12-Nov-2022	10	** UNSUPPORTED WHEN ASSIGNED ** A remote unauthenticated insecure deserialization vulnerability exists in VMware Hyperic Server 5.8.6. Exploitation of this vulnerability enables a malicious party to run arbitrary code or malware within Hyperic Server and the host operating system with the privileges of the Hyperic server process. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2022-38650**	N/A	A-VMW-HYPE-221122/1054
Product: spring_boot_tools					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.40.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	04-Nov-2022	9.8	Spring Tools 4 for Eclipse version 4.16.0 and below as well as VSCode extensions such as Spring Boot Tools, Concourse CI Pipeline Editor, Bosh Editor and Cloudfoundry Manifest YML Support version 1.39.0 and below all use Snakeyaml library for YAML editing support. This library allows for some special syntax in the YAML that under certain circumstances allows for potentially harmful remote code execution by the attacker. **CVE ID : CVE-2022-31691**	https://tanzu.vmware.com/security/cve-2022-31691	A-VMW-SPRI-221122/1055
Product: spring_tools					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.16.1					
Improper Control of Generation of Code ('Code Injection')	04-Nov-2022	9.8	Spring Tools 4 for Eclipse version 4.16.0 and below as well as VSCode extensions such as Spring Boot Tools, Concourse CI Pipeline Editor, Bosh Editor and Cloudfoundry Manifest YML Support version 1.39.0 and below all	https://tanzu.vmware.com/security/cve-2022-31691	A-VMW-SPRI-221122/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use Snakeyaml library for YAML editing support. This library allows for some special syntax in the YAML that under certain circumstances allows for potentially harmful remote code execution by the attacker. **CVE ID : CVE-2022-31691**		
Product: workspace_one_assist					
Affected Version(s): * Up to (excluding) 22.10					
Missing Authentication for Critical Function	09-Nov-2022	9.8	VMware Workspace ONE Assist prior to 22.10 contains an Authentication Bypass vulnerability. A malicious actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application. **CVE ID : CVE-2022-31685**	https://www.vmware.com/security/advisories/VMSA-2022-0028.html	A-VMW-WORK-221122/1057
Improper Authentication	09-Nov-2022	9.8	VMware Workspace ONE Assist prior to 22.10 contains a Broken	https://www.vmware.com/security/advisories/VMSA-	A-VMW-WORK-221122/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Authentication Method vulnerability. A malicious actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application. **CVE ID : CVE-2022-31686**	2022-0028.html	
N/A	09-Nov-2022	9.8	VMware Workspace ONE Assist prior to 22.10 contains a Broken Access Control vulnerability. A malicious actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application. **CVE ID : CVE-2022-31687**	https://www.vmware.com/security/advisories/VMSA-2022-0028.html	A-VMW-WORK-221122/1059
Session Fixation	09-Nov-2022	9.8	VMware Workspace ONE Assist prior to 22.10 contains a Session fixation vulnerability. A malicious actor	https://www.vmware.com/security/advisories/VMSA-2022-0028.html	A-VMW-WORK-221122/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			who obtains a valid session token may be able to authenticate to the application using that token. **CVE ID : CVE-2022-31689**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Nov-2022	6.1	VMware Workspace ONE Assist prior to 22.10 contains a Reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31688**	https://www.vmware.com/security/advisories/VMSA-2022-0028.html	A-VMW-WORK-221122/1061
Vendor: vr_calendar_project					
Product: vr_calendar					
Affected Version(s): * Up to (excluding) 2.3.4					
Cross-Site Request Forgery (CSRF)	03-Nov-2022	6.5	The VR Calendar plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.3.3. This is due to missing or incorrect nonce validation on several functions.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2809350%40vr-calendar-sync&new=2809350%40vr-calendar-sync&sfp_ema	A-VR_-VR_C-221122/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This makes it possible for unauthenticated attackers to delete, and modify calendars as well as the plugin settings, via forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2022-3852**	il=&sfph_mail=	
Vendor: watchdog					
Product: anti-virus					
Affected Version(s): 1.4.158					
N/A	04-Nov-2022	6.5	Incorrect access control in the anti-virus driver wsdkd.sys of Watchdog Antivirus v1.4.158 allows attackers to write arbitrary files. **CVE ID : CVE-2022-38582**	N/A	A-WAT-ANTI-221122/1063
Vendor: web-based_student_clearance_system_project					
Product: web-based_student_clearance_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	01-Nov-2022	4.8	A cross-site scripting (XSS) vulnerability in /admin/edit-admin.php of Web-Based Student Clearance System v1.0 allows attackers to execute	N/A	A-WEB-WEB--221122/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			arbitrary web scripts or HTML via a crafted payload injected into the txtemail parameter. **CVE ID : CVE-2022-43076**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Nov-2022	4.8	A cross-site scripting (XSS) vulnerability in /admin/add-fee.php of Web-Based Student Clearance System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cmddept parameter. **CVE ID : CVE-2022-43078**	N/A	A-WEB-WEB--221122/1065
Vendor: webartesanal					
Product: mantenimiento_web					
Affected Version(s): * Up to (including) 0.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Mantenimiento web plugin <= 0.13 on WordPress. **CVE ID : CVE-2022-41980**	https://patchstack.com/database/vulnerability/mantenimiento-web/wordpress-mantenimiento-web-plugin-0-13-auth-cross-site-scripting-xss-vulnerability?_s_id=cve, https://word	A-WEB-MANT-221122/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				press.org/plugins/mantenimiento-web/	
Vendor: weberge					
Product: wp_hide					
Affected Version(s): * Up to (including) 0.0.2					
Cross-Site Request Forgery (CSRF)	07-Nov-2022	5.3	The WP Hide WordPress plugin through 0.0.2 does not have authorisation and CSRF checks in place when updating the custom_wpadmin_slug settings, allowing unauthenticated attackers to update it with a crafted request **CVE ID : CVE-2022-3489**	https://wpscan.com/vulnerability/36d78b6c-0da5-44f8-b7b3-eae78edac505	A-WEB-WP_H-221122/1067
Vendor: webmaster_tools_verification_project					
Product: webmaster_tools_verification					
Affected Version(s): * Up to (including) 1.2					
Cross-Site Request Forgery (CSRF)	14-Nov-2022	6.5	The Webmaster Tools Verification WordPress plugin through 1.2 does not have authorisation and CSRF checks when disabling plugins, allowing unauthenticated users to disable arbitrary plugins **CVE ID : CVE-2022-3538**	https://wpscan.com/vulnerability/337ee7ed-9ade-4567-b976-88386cbcf036	A-WEB-WEBM-221122/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Webmin					
Product: webmin					
Affected Version(s): * Up to (excluding) 2022-10-30					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Nov-2022	6.1	A vulnerability, which was classified as problematic, was found in Webmin. Affected is an unknown function of the file xterm/index.cgi. The manipulation leads to basic cross site scripting. It is possible to launch the attack remotely. The name of the patch is d3d33af3c0c3fd3a889c84e287a038b7a457d811. It is recommended to apply a patch to fix this issue. VDB-212862 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3844**	https://github.com/webmin/webmin/commit/d3d33af3c0c3fd3a889c84e287a038b7a457d811	A-WEB-WEBM-221122/1069
Vendor: Wolfssl					
Product: wolfssl					
Affected Version(s): * Up to (excluding) 5.5.2					
Out-of-bounds Read	07-Nov-2022	9.1	In wolfSSL before 5.5.2, if callback functions are enabled (via the WOLFSSL_CALLBACKS flag), then a malicious TLS 1.3	https://www.wolfssl.com/docs/security-vulnerabilities/	A-WOL-WOLF-221122/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			client or network attacker can trigger a buffer over-read on the heap of 5 bytes. (WOLFSSL_CALLBACKS is only intended for debugging.) **CVE ID : CVE-2022-42905**		
Vendor: wowonder					
Product: wowonder					
Affected Version(s): 4.1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Nov-2022	7.5	WoWonder Social Network Platform v4.1.2 was discovered to contain a SQL injection vulnerability via the offset parameter at requests.php?f=load-my-blogs. **CVE ID : CVE-2022-40405**	N/A	A-WOW-WOWO-221122/1071
Affected Version(s): 4.1.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Nov-2022	9.8	WoWonder Social Network Platform 4.1.4 was discovered to contain a SQL injection vulnerability via the offset parameter at requests.php?f=search&s=recipients. **CVE ID : CVE-2022-42984**	https://www.wowonder.com/	A-WOW-WOWO-221122/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wpadvancedads					
Product: advanced_ads_-_ad_manager_\&_adsense					
Affected Version(s): * Up to (excluding) 1.32.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Advanced Ads GmbH Advanced Ads – Ad Manager & AdSense plugin <= 1.31.1 on WordPress. **CVE ID : CVE-2022-32776**	https://patchstack.com/database/vulnerability/advanced-ads/wordpress-advanced-ads-ad-manager-adsense-plugin-1-31-1-authenticated-stored-cross-site-scripting-xss-vulnerability?_s_id=cve, https://wordpress.org/plugins/advanced-ads/	A-WPA-ADVA-221122/1073
Vendor: wpb_show_core_project					
Product: wpb_show_core					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	6.1	The WPB Show Core WordPress plugin through TODO does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-3484**	https://wpscan.com/vulnerability/3afaed61-6187-4915-acf0-16e79d5c2464	A-WPB-WPB_-221122/1074
Vendor: wpforms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wpforms_pro					
Affected Version(s): * Up to (excluding) 1.7.7					
Improper Neutralization of Formula Elements in a CSV File	14-Nov-2022	9.8	The WPForms Pro WordPress plugin before 1.7.7 does not validate its form data when generating the exported CSV, which could lead to CSV injection. **CVE ID : CVE-2022-3574**	https://wpscan.com/vulnerability/0eae5189-81af-4344-9e96-dd1f4e223d41	A-WPF-WPFO-221122/1075
Vendor: wp_attachments_project					
Product: wp_attachments					
Affected Version(s): * Up to (excluding) 5.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Nov-2022	4.8	The WP Attachments WordPress plugin before 5.0.5 does not sanitize and escapes 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-2022-3469**	https://wpscan.com/vulnerability/017ca231-e019-4694-afa2-ab7f8481ae63	A-WP_-WP_A-221122/1076
Vendor: wsgidav_project					
Product: wsgidav					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 4.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	6.1	WsgiDAV is a generic and extendable WebDAV server based on WSGI. Implementations using this library with directory browsing enabled may be susceptible to Cross Site Scripting (XSS) attacks. This issue has been patched, users can upgrade to version 4.1.0. As a workaround, set `dir_browser.enable = False` in the configuration. **CVE ID : CVE-2022-41905**	https://github.com/mar10/wsgidav/commit/e9606ab0f42f4c1a6611bc3c52de299b0aba7726, https://github.com/mar10/wsgidav/security/advisories/GHSA-xx6g-jj35-pxjv	A-WSG-WSGI-221122/1077
Vendor: Xfce					
Product: xfce4-settings					
Affected Version(s): * Up to (excluding) 4.16.4					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	09-Nov-2022	9.8	In Xfce xfce4-settings before 4.16.4 and 4.17.x before 4.17.1, there is an argument injection vulnerability in xfce4-mime-helper. **CVE ID : CVE-2022-45062**	https://gitlab.xfce.org/xfce/xfce4-settings/-/commit/55e3c5fb667e96ad1412cf249879262b369d28d7, https://gitlab.xfce.org/xfce/xfce4-settings/-/commit/f34a92a84f96268ad24a7a13fd5edc9f1d52611	A-XFC-XFCE-221122/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				0, https://gitlab.xfce.org/xfce/xfce4-settings/-/tags	
Affected Version(s): 4.17.0					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	09-Nov-2022	9.8	In Xfce xfce4-settings before 4.16.4 and 4.17.x before 4.17.1, there is an argument injection vulnerability in xfce4-mime-helper. **CVE ID : CVE-2022-45062**	https://gitlab.xfce.org/xfce/xfce4-settings/-/commit/55e3c5fb667e96ad1412cf249879262b369d28d7, https://gitlab.xfce.org/xfce/xfce4-settings/-/commit/f34a92a84f96268ad24a7a13fd5edc9f1d526110, https://gitlab.xfce.org/xfce/xfce4-settings/-/tags	A-XFC-XFCE-221122/1079
Vendor: xmldom_project					
Product: xmldom					
Affected Version(s): * Up to (excluding) 0.6.0					
Improper Input Validation	02-Nov-2022	9.8	xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) `DOMParser` and `XMLSerializer` module. xmldom parses XML that is not well-formed	https://github.com/xmldom/xmldom/security/advisories/GHSA-crh6-fp67-6883	A-XML-XMLD-221122/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because it contains multiple top level elements, and adds all root nodes to the `childNodes` collection of the `Document`, without reporting any error or throwing. This breaks the assumption that there is only a single root node in the tree, which led to issuance of CVE-2022-39299 as it is a potential issue for dependents. Update to @xmldom/xmldom @~0.7.7, @xmldom/xmldom @~0.8.4 (dist-tag latest) or @xmldom/xmldom @>=0.9.0-beta.4 (dist-tag next). As a workaround, please one of the following approaches depending on your use case: instead of searching for elements in the whole DOM, only search in the `documentElement` or reject a document with a document that has more then 1 `childNode`.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39353		
Affected Version(s): 0.9.0					
Improper Input Validation	02-Nov-2022	9.8	xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) `DOMParser` and `XMLSerializer` module. xmldom parses XML that is not well-formed because it contains multiple top level elements, and adds all root nodes to the `childNodes` collection of the `Document`, without reporting any error or throwing. This breaks the assumption that there is only a single root node in the tree, which led to issuance of CVE-2022-39299 as it is a potential issue for dependents. Update to @xmldom/xmldom @~0.7.7, @xmldom/xmldom @~0.8.4 (dist-tag latest) or @xmldom/xmldom @>=0.9.0-beta.4 (dist-tag next). As a workaround, please one of the following approaches	https://github.com/xmldom/xmldom/security/advisories/GHSA-crh6-fp67-6883	A-XML-XMLD-221122/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			depending on your use case: instead of searching for elements in the whole DOM, only search in the `documentElement` or reject a document with a document that has more then 1 `childNode`. **CVE ID : CVE-2022-39353**		
Affected Version(s): From (including) 0.7.0 Up to (excluding) 0.7.7					
Improper Input Validation	02-Nov-2022	9.8	xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) `DOMParser` and `XMLSerializer` module. xmldom parses XML that is not well-formed because it contains multiple top level elements, and adds all root nodes to the `childNodes` collection of the `Document`, without reporting any error or throwing. This breaks the assumption that there is only a single root node in the tree, which led to issuance of CVE-2022-39299 as it is a potential issue for dependents. Update	https://github.com/xmldom/xmldom/security/advisories/GHSA-crh6-fp67-6883	A-XML-XMLD-221122/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to @xmldom/xmldom @~0.7.7, @xmldom/xmldom @~0.8.4 (dist-tag latest) or @xmldom/xmldom @>=0.9.0-beta.4 (dist-tag next). As a workaround, please one of the following approaches depending on your use case: instead of searching for elements in the whole DOM, only search in the `documentElement` or reject a document with a document that has more then 1 `childNode`. **CVE ID : CVE-2022-39353**		
Affected Version(s): From (including) 0.8.0 Up to (excluding) 0.8.4					
Improper Input Validation	02-Nov-2022	9.8	xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) `DOMParser` and `XMLSerializer` module. xmldom parses XML that is not well-formed because it contains multiple top level elements, and adds all root nodes to the `childNodes` collection of the `Document`,	https://github.com/xmldom/xmldom/security/advisories/GHSA-crh6-fp67-6883	A-XML-XMLD-221122/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without reporting any error or throwing. This breaks the assumption that there is only a single root node in the tree, which led to issuance of CVE-2022-39299 as it is a potential issue for dependents. Update to @xmldom/xmldom @~0.7.7, @xmldom/xmldom @~0.8.4 (dist-tag latest) or @xmldom/xmldom @>=0.9.0-beta.4 (dist-tag next). As a workaround, please one of the following approaches depending on your use case: instead of searching for elements in the whole DOM, only search in the `documentElement` or reject a document with a document that has more then 1 `childNode`. **CVE ID : CVE-2022-39353**		
Vendor: xpdfreader					
Product: xpdf					
Affected Version(s): 4.04					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	14-Nov-2022	5.5	XPDF v4.04 was discovered to contain a stack overflow via the function FileStream::copy() at xpdf/Stream.cc:795. **CVE ID : CVE-2022-43295**	https://forum.xpdfreader.com/viewtopic.php?t=42360	A-XPD-XPDF-221122/1084
Vendor: Xwiki					
Product: openid_connect					
Affected Version(s): * Up to (excluding) 1.29.1					
Improper Authentication	04-Nov-2022	7.5	XWiki OIDC has various tools to manipulate OpenID Connect protocol in XWiki. Prior to version 1.29.1, even if a wiki has an OpenID provider configured through its xwiki.properties, it is possible to provide a third party provider its details through request parameters. One can then bypass the XWiki authentication altogether by specifying its own provider through the oidc.endpoint.* request parameters (or by using an XWiki-based OpenID provider with	https://jira.xwiki.org/browse/OIDC-118, https://github.com/xwiki-contrib/oidc/security/advisories/GHSA-m7gv-v8xx-v47w, https://github.com/xwiki-contrib/oidc/commit/0247af1417925b9734ab106ad7cd934ee870ac89	A-XWI-OPEN-221122/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			oidc.xwikiprovider. With the same approach, one could also provide a specific group mapping through oidc.groups.mapping that would make his user automatically part of the XWikiAdminGroup. This issue has been patched, please upgrade to 1.29.1. There is no workaround, an upgrade of the authenticator is required. **CVE ID : CVE-2022-39387**		
Vendor: zettlr					
Product: zettlr					
Affected Version(s): 2.3.0					
Improper Input Validation	03-Nov-2022	5.5	Zettlr version 2.3.0 allows an external attacker to remotely obtain arbitrary local files on any client that attempts to view a malicious markdown file through Zettlr. This is possible because the application does not have a CSP policy (or at least not strict enough) and/or does not properly validate	N/A	A-ZET-ZETT-221122/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the contents of markdown files before rendering them. **CVE ID : CVE-2022-40276**		
Vendor: zkteco					
Product: biotime					
Affected Version(s): 8.5.4					
Missing Authentication for Critical Function	08-Nov-2022	5.3	ZKTeco BioTime 8.5.4 is missing authentication on folders containing employee photos, allowing an attacker to view them through filename enumeration. **CVE ID : CVE-2022-30515**	https://www.zkteco.me/software-5	A-ZKT-BIOT-221122/1087
Affected Version(s): 8.5.5					
Missing Authentication for Critical Function	08-Nov-2022	5.3	ZKTeco BioTime 8.5.4 is missing authentication on folders containing employee photos, allowing an attacker to view them through filename enumeration. **CVE ID : CVE-2022-30515**	https://www.zkteco.me/software-5	A-ZKT-BIOT-221122/1088
Vendor: Zohocorp					
Product: manageengine_access_manager_plus					
Affected Version(s): 4.3					
Improper Neutralizat	12-Nov-2022	9.8	Zoho ManageEngine	https://www.manageengine	A-ZOH-MANA-221122/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection. **CVE ID : CVE-2022-43671**	.com/products/passwordmanagerpro/advisory/cve-2022-43671.html	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection (in a different software component relative to CVE-2022-43671. **CVE ID : CVE-2022-43672**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-43672.html	A-ZOH-MANA-221122/1090
Affected Version(s): * Up to (excluding) 4.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection. **CVE ID : CVE-2022-43671**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-43671.html	A-ZOH-MANA-221122/1091
Improper Neutralization of Special Elements used in an	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-	A-ZOH-MANA-221122/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			Manager Plus before 4306 allow SQL Injection (in a different software component relative to CVE-2022-43671. **CVE ID : CVE-2022-43672**	2022-43672.html	
Product: manageengine_mobile_device_manager_plus					
Affected Version(s): 10.1.2207.4					
N/A	12-Nov-2022	7.8	In Zoho ManageEngine Mobile Device Manager Plus before 10.1.2207.5, the User Administration module allows privilege escalation. **CVE ID : CVE-2022-41339**	https://www.manageengine.com/mobile-device-management/kb/CVE-2022-41339.html	A-ZOH-MANA-221122/1093
Product: manageengine_pam360					
Affected Version(s): * Up to (excluding) 5.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection. **CVE ID : CVE-2022-43671**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-43671.html	A-ZOH-MANA-221122/1094
Improper Neutralization of Special Elements used in an	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-	A-ZOH-MANA-221122/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			Manager Plus before 4306 allow SQL Injection (in a different software component relative to CVE-2022-43671. **CVE ID : CVE-2022-43672**	2022-43672.html	
Affected Version(s): 5.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection. **CVE ID : CVE-2022-43671**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-43671.html	A-ZOH-MANA-221122/1096
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection (in a different software component relative to CVE-2022-43671. **CVE ID : CVE-2022-43672**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-43672.html	A-ZOH-MANA-221122/1097
Product: manageengine_password_manager_pro					
Affected Version(s): * Up to (excluding) 12.1					
Improper Neutralization of	12-Nov-2022	9.8	Zoho ManageEngine Password Manager	https://www.manageengine.com/product	A-ZOH-MANA-221122/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection. **CVE ID : CVE-2022-43671**	s/passwordmanagerpro/advisory/cve-2022-43671.html	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection (in a different software component relative to CVE-2022-43671. **CVE ID : CVE-2022-43672**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-43672.html	A-ZOH-MANA-221122/1099
Affected Version(s): 12.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection. **CVE ID : CVE-2022-43671**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-43671.html	A-ZOH-MANA-221122/1100
Improper Neutralization of Special Elements used in an SQL	12-Nov-2022	9.8	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-	A-ZOH-MANA-221122/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			before 4306 allow SQL Injection (in a different software component relative to CVE-2022-43671. **CVE ID : CVE-2022-43672**	2022-43672.html	
Product: manageengine_servicedesk_plus_msp					
Affected Version(s): * Up to (excluding) 10.6					
Incorrect Authorization	12-Nov-2022	8.8	Zoho ManageEngine ServiceDesk Plus MSP before 10609 and SupportCenter Plus before 11025 are vulnerable to privilege escalation. This allows users to obtain sensitive data during an exportMickeyList export of requests from the list view. **CVE ID : CVE-2022-40773**	https://www.manageengine.com/products/service-desk-msp/cve-2022-40773.html	A-ZOH-MANA-221122/1102
Affected Version(s): 10.6					
Incorrect Authorization	12-Nov-2022	8.8	Zoho ManageEngine ServiceDesk Plus MSP before 10609 and SupportCenter Plus before 11025 are vulnerable to privilege escalation. This allows users to obtain sensitive data during an exportMickeyList export of requests from the list view.	https://www.manageengine.com/products/service-desk-msp/cve-2022-40773.html	A-ZOH-MANA-221122/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40773		
Product: manageengine_supportcenter_plus					
Affected Version(s): * Up to (excluding) 11.0					
Incorrect Authorization	12-Nov-2022	8.8	Zoho ManageEngine ServiceDesk Plus MSP before 10609 and SupportCenter Plus before 11025 are vulnerable to privilege escalation. This allows users to obtain sensitive data during an exportMickeyList export of requests from the list view. **CVE ID : CVE-2022-40773**	https://www.manageengine.com/products/service-desk-msp/cve-2022-40773.html	A-ZOH-MANA-221122/1104
Affected Version(s): 11.0					
Incorrect Authorization	12-Nov-2022	8.8	Zoho ManageEngine ServiceDesk Plus MSP before 10609 and SupportCenter Plus before 11025 are vulnerable to privilege escalation. This allows users to obtain sensitive data during an exportMickeyList export of requests from the list view. **CVE ID : CVE-2022-40773**	https://www.manageengine.com/products/service-desk-msp/cve-2022-40773.html	A-ZOH-MANA-221122/1105
Product: zoho_crm_lead_magnet					
Affected Version(s): * Up to (including) 1.7.5.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	6.5	Auth. (subscriber+) Arbitrary Options Update vulnerability in Zoho CRM Lead Magnet plugin <= 1.7.5.8 on WordPress. **CVE ID : CVE-2022-41978**	https://wordpress.org/plugins/zoho-crm-forms/#developers, https://patchstack.com/database/vulnerability/zoho-crm-forms/wordpress-zoho-crm-lead-magnet-plugin-1-7-5-6-auth-arbitrary-options-update-vulnerability?_s_id=cve	A-ZOH-ZOHO-221122/1106
Vendor: Zoneminder					
Product: Zoneminder					
Affected Version(s): * Up to (including) 1.36.12					
Session Fixation	15-Nov-2022	4.6	Session fixation exists in ZoneMinder through 1.36.12 as an attacker can poison a session cookie to the next logged-in user. **CVE ID : CVE-2022-30769**	N/A	A-ZON-ZONE-221122/1107
Vendor: ZTE					
Product: zaip-aie					
Affected Version(s): * Up to (excluding) 8.22.02					
Improper Neutralization of Special	08-Nov-2022	5.3	There is a SQL injection vulnerability in ZTE ZAIP-AIE. Due to	https://support.zte.com.cn/support/news/LoopholeInfo	A-ZTE-ZAIP-221122/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			lack of input verification by the server, an attacker could trigger an attack by building malicious requests. Exploitation of this vulnerability could cause the leakage of the current table content. **CVE ID : CVE-2022-39069**	Detail.aspx?newsId=1026604	
Hardware					
Vendor: AMD					
Product: a10-9600p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-A10--221122/1109
Product: a10-9630p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	H-AMD-A10--221122/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	security/2022/11/10/2	
Product: a12-9700p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-A12--221122/1111
Product: a12-9730p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-A12--221122/1112
Product: a4-9120					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	H-AMD-A4-9-221122/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: a6-9210					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-A6-9-221122/1114
Product: a6-9220					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-A6-9-221122/1115
Product: a6-9220c					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	H-AMD-A6-9-221122/1116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: a9-9410					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-A9-9-221122/1117
Product: a9-9420					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-A9-9-221122/1118
Product: athlon_gold_3150u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	H-AMD-ATHL-221122/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: athlon_silver_3050u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1120
Product: athlon_x4_750					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1121
Product: athlon_x4_760k					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1122
Product: athlon_x4_830					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1123
Product: athlon_x4_835					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: athlon_x4_840					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1125
Product: athlon_x4_845					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1126
Product: athlon_x4_860k					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	H-AMD-ATHL-221122/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: athlon_x4_870k					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1128
Product: athlon_x4_880k					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1129
Product: athlon_x4_940					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	H-AMD-ATHL-221122/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: athlon_x4_950					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1131
Product: athlon_x4_970					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-ATHL-221122/1132
Product: epyc_7001					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	H-AMD-EPYC-221122/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7002					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1134
Product: epyc_7003					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1135
Product: epyc_7251					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-221122/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7252					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1137
Product: epyc_7261					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1138
Product: epyc_7262					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	H-AMD-EPYC-221122/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7272					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1140
Product: epyc_7281					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1141
Product: epyc_7282					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1142
Product: epyc_72f3					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1143
Product: epyc_7301					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: epyc_7302					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1145
Product: epyc_7302p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1146
Product: epyc_7313					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	H-AMD-EPYC-221122/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: epyc_7313p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1148
Product: epyc_7343					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1149
Product: epyc_7351					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	H-AMD-EPYC-221122/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7351p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1151
Product: epyc_7352					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1152
Product: epyc_7371					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	H-AMD-EPYC-221122/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7373x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1154
Product: epyc_7401					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1155
Product: epyc_7401p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-221122/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7402					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1157
Product: epyc_7402p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1158
Product: epyc_7413					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	H-AMD-EPYC-221122/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7443					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1160
Product: epyc_7443p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1161
Product: epyc_7451					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1162
Product: epyc_7452					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1163
Product: epyc_7473x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: epyc_74f3					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1165
Product: epyc_7501					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1166
Product: epyc_7502					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	H-AMD-EPYC-221122/1167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: epyc_7502p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1168
Product: epyc_7513					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1169
Product: epyc_7532					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	H-AMD-EPYC-221122/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7542					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1171
Product: epyc_7543					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1172
Product: epyc_7543p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	H-AMD-EPYC-221122/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7551					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1174
Product: epyc_7551p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1175
Product: epyc_7552					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	H-AMD-EPYC-221122/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7573x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1177
Product: epyc_75f3					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1178
Product: epyc_7601					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	H-AMD-EPYC-221122/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7642					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1180
Product: epyc_7643					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1181
Product: epyc_7662					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1182
Product: epyc_7663					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1183
Product: epyc_7702					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: epyc_7713					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1185
Product: epyc_7713p					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1186
Product: epyc_7742					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	H-AMD-EPYC-221122/1187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: epyc_7763					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1188
Product: epyc_7773x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1189
Product: epyc_7f32					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	H-AMD-EPYC-221122/1190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7f52					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1191
Product: epyc_7f72					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-EPYC-221122/1192
Product: epyc_7h12					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	H-AMD-EPYC-221122/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_3_2200u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1194
Product: ryzen_3_2300u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1195
Product: ryzen_3_3100					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	H-AMD-RYZE-221122/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_3_3200u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1197
Product: ryzen_3_3250u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1198
Product: ryzen_3_3300g					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	H-AMD-RYZE-221122/1199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_3_3300u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1200
Product: ryzen_3_3300x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1201
Product: ryzen_3_4300g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1202
Product: ryzen_3_4300ge					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1203
Product: ryzen_3_4300u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ryzen_3_5125c					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1205
Product: ryzen_3_5400u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1206
Product: ryzen_3_5425c					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	H-AMD-RYZE-221122/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: ryzen_3_5425u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1208
Product: ryzen_5_2500u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1209
Product: ryzen_5_2600					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	H-AMD-RYZE-221122/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_2600h					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1211
Product: ryzen_5_2600x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1212
Product: ryzen_5_2700					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	H-AMD-RYZE-221122/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_2700x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1214
Product: ryzen_5_3400g					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1215
Product: ryzen_5_3450g					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	H-AMD-RYZE-221122/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_3500u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1217
Product: ryzen_5_3550h					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1218
Product: ryzen_5_3580u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	H-AMD-RYZE-221122/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_3600					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1220
Product: ryzen_5_3600x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1221
Product: ryzen_5_3600xt					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1222
Product: ryzen_5_4500u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1223
Product: ryzen_5_4600g					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ryzen_5_4600ge					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1225
Product: ryzen_5_4600h					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1226
Product: ryzen_5_4600u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	H-AMD-RYZE-221122/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: ryzen_5_5560u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1228
Product: ryzen_5_5600h					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1229
Product: ryzen_5_5600hs					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	H-AMD-RYZE-221122/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_5600u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1231
Product: ryzen_5_5625c					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1232
Product: ryzen_5_5625u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	H-AMD-RYZE-221122/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_7_2700					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1234
Product: ryzen_7_2700u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1235
Product: ryzen_7_2700x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	H-AMD-RYZE-221122/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_7_2800h					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1237
Product: ryzen_7_3700u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1238
Product: ryzen_7_3700x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	H-AMD-RYZE-221122/1239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_7_3750h					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1240
Product: ryzen_7_3780u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1241
Product: ryzen_7_3800x					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1242
Product: ryzen_7_3800xt					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1243
Product: ryzen_7_4700g					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ryzen_7_4700ge					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1245
Product: ryzen_7_4700u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1246
Product: ryzen_7_4800h					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	H-AMD-RYZE-221122/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: ryzen_7_4800u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1248
Product: ryzen_7_5800h					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1249
Product: ryzen_7_5800hs					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	H-AMD-RYZE-221122/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_7_5800u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1251
Product: ryzen_7_5825c					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1252
Product: ryzen_7_5825u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	H-AMD-RYZE-221122/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_7_pro_3700u					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1254
Product: ryzen_9_4900h					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1255
Product: ryzen_9_5900hs					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	H-AMD-RYZE-221122/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_9_5900hx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1257
Product: ryzen_9_5980hs					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1258
Product: ryzen_9_5980hx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	H-AMD-RYZE-221122/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_threadripper_2920x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1260
Product: ryzen_threadripper_2950x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1261
Product: ryzen_threadripper_2970wx					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1262
Product: ryzen_threadripper_2990wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1263
Product: ryzen_threadripper_3960x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ryzen_threadripper_3970x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1265
Product: ryzen_threadripper_3990x					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1266
Product: ryzen_threadripper_pro_3795wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	H-AMD-RYZE-221122/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: ryzen_threadripper_pro_3945wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1268
Product: ryzen_threadripper_pro_3955wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1269
Product: ryzen_threadripper_pro_3995wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	H-AMD-RYZE-221122/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_threadripper_pro_5945wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1271
Product: ryzen_threadripper_pro_5955wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1272
Product: ryzen_threadripper_pro_5965wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	H-AMD-RYZE-221122/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_threadripper_pro_5975wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1274
Product: ryzen_threadripper_pro_5995wx					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	H-AMD-RYZE-221122/1275
Vendor: Avaya					
Product: scopia_pathfinder_10_pts					
Affected Version(s): -					
Missing Authentica	03-Nov-2022	9.1	** UNSUPPPORTED WHEN ASSIGNED	N/A	H-AVA-SCOP-221122/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion for Critical Function			**Broken Access Control in User Authentication in Avaya Scopia Pathfinder 10 and 20 PTS version 8.3.7.0.4 allows remote unauthenticated attackers to bypass the login page, access sensitive information, and reset user passwords via URL modification. **CVE ID : CVE-2022-38168**		
Product: scopia_pathfinder_20_pts					
Affected Version(s): -					
Missing Authentication for Critical Function	03-Nov-2022	9.1	** UNSUPPPORTED WHEN ASSIGNED **Broken Access Control in User Authentication in Avaya Scopia Pathfinder 10 and 20 PTS version 8.3.7.0.4 allows remote unauthenticated attackers to bypass the login page, access sensitive information, and reset user passwords via URL modification. **CVE ID : CVE-2022-38168**	N/A	H-AVA-SCOP-221122/1277
Vendor: BD					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: totalys_multiprocessor					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Nov-2022	7.8	BD Totalys MultiProcessor, versions 1.70 and earlier, contain hardcoded credentials. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII). Customers using BD Totalys MultiProcessor version 1.70 with Microsoft Windows 10 have additional operating system hardening configurations which increase the attack complexity required to exploit this vulnerability. **CVE ID : CVE-2022-40263**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-totalys-multiprocessor-hardcoded-credentials	H-BD-TOTA-221122/1278
Vendor: Cisco					
Product: email_security_appliance					
Affected Version(s): -					
Improper Neutralization of	04-Nov-2022	5.3	A vulnerability in Cisco Email Security Appliance	https://tools.cisco.com/security/center/co	H-CIS-EMAI-221122/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			(ESA) and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. This vulnerability is due to the failure of the application or its environment to properly sanitize input values. An attacker could exploit this vulnerability by injecting malicious HTTP headers, controlling the response body, or splitting the response into multiple responses. **CVE ID : CVE-2022-20772**	ntent/CiscoSecurityAdvisory/cisco-sa-ESA-HTTP-Inject-nvsycUmR	
Product: secure_email_and_web_manager					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Email Security Appliance, Cisco Secure Email and Web Manager and Cisco Secure Web Appliance could allow an authenticated, remote attacker to elevate privileges	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	H-CIS-SECU-221122/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on an affected system. The attacker needs valid credentials to exploit this vulnerability. This vulnerability is due to the use of a hardcoded value to encrypt a token used for certain APIs calls . An attacker could exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to impersonate another valid user and execute commands with the privileges of that user account. **CVE ID : CVE-2022-20868**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Nov-2022	6.5	A vulnerability in web-based management interface of the of Cisco Email Security Appliance and Cisco Secure Email and Web Manager could allow an authenticated, remote attacker to conduct SQL	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	H-CIS-SECU-221122/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection attacks as root on an affected system. The attacker must have the credentials of a high-privileged user account. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database of the affected system. **CVE ID : CVE-2022-20867**		
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA),	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	H-CIS-SECU-221122/1282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, remote attacker to retrieve sensitive information from an affected device, including user credentials. This vulnerability is due to weak enforcement of back-end authorization checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Nov-2022	5.3	A vulnerability in Cisco Email Security Appliance (ESA) and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. This vulnerability is due to the failure of the application or its environment to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-HTTP-Inject-nvsycUmR	H-CIS-SECU-221122/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly sanitize input values. An attacker could exploit this vulnerability by injecting malicious HTTP headers, controlling the response body, or splitting the response into multiple responses. **CVE ID : CVE-2022-20772**		
Product: secure_email_gateway					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Email Security Appliance, Cisco Secure Email and Web Manager and Cisco Secure Web Appliance could allow an authenticated, remote attacker to elevate privileges on an affected system. The attacker needs valid credentials to exploit this vulnerability. This vulnerability is due to the use of a hardcoded value to encrypt a token used for certain APIs calls . An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	H-CIS-SECU-221122/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to impersonate another valid user and execute commands with the privileges of that user account. **CVE ID : CVE-2022-20868**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Nov-2022	6.5	A vulnerability in web-based management interface of the of Cisco Email Security Appliance and Cisco Secure Email and Web Manager could allow an authenticated, remote attacker to conduct SQL injection attacks as root on an affected system. The attacker must have the credentials of a high-privileged user account. This vulnerability is due to improper validation of user-submitted parameters. An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	H-CIS-SECU-221122/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database of the affected system. **CVE ID : CVE-2022-20867**		
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive information from an affected device, including user credentials. This vulnerability is due to weak enforcement of back-end authorization	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	H-CIS-SECU-221122/1286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Product: secure_web_appliance					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Email Security Appliance, Cisco Secure Email and Web Manager and Cisco Secure Web Appliance could allow an authenticated, remote attacker to elevate privileges on an affected system. The attacker needs valid credentials to exploit this vulnerability. This vulnerability is due to the use of a hardcoded value to encrypt a token used for certain APIs calls . An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	H-CIS-SECU-221122/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to impersonate another valid user and execute commands with the privileges of that user account. **CVE ID : CVE-2022-20868**		
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive information from an affected device, including user credentials. This vulnerability is due to weak enforcement of back-end authorization	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	H-CIS-SECU-221122/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Vendor: Citrix					
Product: application_delivery_controller					
Affected Version(s): -					
Improper Authentication	08-Nov-2022	9.8	Unauthorized access to Gateway user capabilities **CVE ID : CVE-2022-27510**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	H-CIT-APPL-221122/1289
Improper Restriction of Excessive Authentication Attempts	08-Nov-2022	9.8	User login brute force protection functionality bypass **CVE ID : CVE-2022-27516**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751	H-CIT-APPL-221122/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				3-and-cve202227516	
Insufficient Verification of Data Authenticity	08-Nov-2022	9.6	Remote desktop takeover via phishing **CVE ID : CVE-2022-27513**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516	H-CIT-APPL-221122/1291
Vendor: Dlink					
Product: dir-823g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Nov-2022	9.8	D-Link DIR-823G v1.0.2 was found to contain a command injection vulnerability in the function SetNetworkTomographySettings. This vulnerability allows attackers to execute arbitrary commands via a crafted packet. **CVE ID : CVE-2022-43109**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--221122/1292
Vendor: inhandnetworks					
Product: inrouter302					
Affected Version(s): -					
N/A	09-Nov-2022	9.8	The firmware of InHand Networks	https://inhandnetworks.co	H-INH-INRO-221122/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InRouter302 V3.5.45 introduces fixes for TALOS-2022-1472 and TALOS-2022-1474. The fixes are incomplete. An attacker can still perform, respectively, a privilege escalation and an information disclosure vulnerability. **CVE ID : CVE-2022-25932**	m/upload/attachment/202210/25/InHand-PSA-2022-02.pdf	
Product: ir302					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	A leftover debug code vulnerability exists in the console support functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-28689**	https://inhandnetworks.com/upload/attachment/202210/25/InHand-PSA-2022-02.pdf	H-INH-IR30-221122/1294
N/A	09-Nov-2022	8.8	A leftover debug code vulnerability exists in the console infct functionality of	https://inhandnetworks.com/upload/attachment/202210/25/InHa	H-INH-IR30-221122/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InHand Networks InRouter302 V3.5.45. A specially-crafted series of network requests can lead to execution of privileged operations. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-30543**	nd-PSA-2022-02.pdf	
N/A	09-Nov-2022	8.1	A leftover debug code vulnerability exists in the httpd port 4444 upload.cgi functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted HTTP request can lead to arbitrary file deletion. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-29888**	https://inhandnetworks.com/upload/attachment/202210/25/InHand-PSA-2022-02.pdf	H-INH-IR30-221122/1296
N/A	09-Nov-2022	6.5	A leftover debug code vulnerability exists in the console verify functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted	https://inhandnetworks.com/upload/attachment/202210/25/InHand-PSA-2022-02.pdf	H-INH-IR30-221122/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series of network requests can lead to disabling security features. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-26023**		
N/A	09-Nov-2022	6.5	A leftover debug code vulnerability exists in the console nvram functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted series of network requests can lead to disabling security features. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-29481**	https://inhandnetworks.com/upload/attachment/202210/25/InHand-PSA-2022-02.pdf	H-INH-IR30-221122/1298
Vendor: Intel					
Product: nuc11dbbi7					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC1-221122/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege via local access. **CVE ID : CVE-2022-38099**		
Product: nuc11dbbi9					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC1-221122/1300
Product: nuc_10_performance_kit_nuc10i3fnh					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i3fnhf					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1302
Product: nuc_10_performance_kit_nuc10i3fnhn					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i3fnk					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1304
Product: nuc_10_performance_kit_nuc10i3fnkn					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i5fnh					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1306
Product: nuc_10_performance_kit_nuc10i5fnhf					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i5fnhj					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1308
Product: nuc_10_performance_kit_nuc10i5fnhn					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i5fnk					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1310
Product: nuc_10_performance_kit_nuc10i5fnkn					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i5fnkp					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1312
Product: nuc_10_performance_kit_nuc10i7fnh					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i7fnhc					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1314
Product: nuc_10_performance_kit_nuc10i7fnhn					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i7fnk					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1316
Product: nuc_10_performance_kit_nuc10i7fnkn					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i7fnkp					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1318
Product: nuc_10_performance_mini_pc_nuc10i3fnhfa					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_mini_pc_nuc10i3fnhja					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1320
Product: nuc_10_performance_mini_pc_nuc10i5fnhca					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_mini_pc_nuc10i5fnhja					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1322
Product: nuc_10_performance_mini_pc_nuc10i5fnkpa					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_mini_pc_nuc10i7fnhaa					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1324
Product: nuc_10_performance_mini_pc_nuc10i7fnhja					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_mini_pc_nuc10i7fnkpa					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1326
Product: nuc_11_compute_element_cm11ebc4w					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1327
Product: nuc_11_compute_element_cm11ebi38w					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1328
Product: nuc_11_compute_element_cm11ebi58w					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1329
Product: nuc_11_compute_element_cm11ebi716w					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version	https://www.intel.com/content/www/us/en/security-center/adviso	H-INT-NUC_-221122/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	ry/intel-sa-00752.html	
Product: nuc_11_compute_element_cm11ebv58w					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1331
Product: nuc_11_compute_element_cm11ebv716w					
Affected Version(s): -					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38099		
Product: nuc_11_performance_kit_nuc11pahi3					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1333
Product: nuc_11_performance_kit_nuc11pahi30z					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_kit_nuc11pahi5					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1335
Product: nuc_11_performance_kit_nuc11pahi50z					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_kit_nuc11pahi7					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1337
Product: nuc_11_performance_kit_nuc11pahi70z					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_kit_nuc11paki3					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1339
Product: nuc_11_performance_kit_nuc11paki5					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_kit_nuc11paki7					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1341
Product: nuc_11_performance_mini_pc_nuc11paqi50wa					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_mini_pc_nuc11paqi70qa					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1343
Product: nuc_11_pro_board_nuc11tnbi30z					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nuc_11_pro_board_nuc11tnbi50z					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1345
Product: nuc_11_pro_board_nuc11tnbi70z					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1346
Product: nuc_11_pro_kit_nuc11tnhi3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1347
Product: nuc_11_pro_kit_nuc11tnhi30z					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1348
Product: nuc_11_pro_kit_nuc11tnhi5					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for	https://www.intel.com/content/www/us/	H-INT-NUC_-221122/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	en/security-center/advisory/intel-sa-00752.html	
Product: nuc_11_pro_kit_nuc11tnhi50z					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1350
Product: nuc_11_pro_kit_nuc11tnhi70z					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro	https://www.intel.com/content/www/us/en/security-center/adviso	H-INT-NUC_-221122/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	ry/intel-sa-00752.html	
Product: nuc_11_pro_kit_nuc11tnki30z					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1352
Product: nuc_11_pro_kit_nuc11tnki50z					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**		
Product: nuc_11_pro_kit_nuc11tnki70z					
Affected Version(s): -					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1354
Product: nuc_8_compute_element_cm8ccb					
Affected Version(s): -					
N/A	11-Nov-2022	6.7	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2022-35276**		
Product: nuc_8_compute_element_cm8i3cb					
Affected Version(s): -					
N/A	11-Nov-2022	6.7	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-35276**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1356
Product: nuc_8_compute_element_cm8i5cb					
Affected Version(s): -					
N/A	11-Nov-2022	6.7	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-35276**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1357
Product: nuc_8_compute_element_cm8i7cb					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Nov-2022	6.7	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-35276**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1358
Product: nuc_8_compute_element_cm8pcb					
Affected Version(s): -					
N/A	11-Nov-2022	6.7	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-35276**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1359
Product: nuc_8_rugged_kit_nuc8cchkr					
Affected Version(s): -					
Incorrect Default Permissions	11-Nov-2022	7.8	Incorrect default permissions in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36377**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Nov-2022	7.8	Path traversal in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36400**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1361
Uncontrolled Search Path Element	11-Nov-2022	7.3	Uncontrolled search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36380**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unquoted Search Path or Element	11-Nov-2022	7.3	Unquoted search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36384**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1363
Product: nuc_board_de3815tybe					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC Boards, Intel(R) NUC Kits before version TY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-34152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1364
Product: nuc_board_nuc5i3mybe					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before	https://www.intel.com/content/www/us/en/security-center/adviso	H-INT-NUC_-221122/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version MYi30060 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36370**	ry/intel-sa-00752.html	
Insecure Default Initialization of Resource	11-Nov-2022	5.5	Insecure default variable initialization in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2022-36349**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1366
Product: nuc_board_nuc8cchb					
Affected Version(s): -					
Incorrect Default Permissions	11-Nov-2022	7.8	Incorrect default permissions in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36377		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Nov-2022	7.8	Path traversal in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36400**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1368
Uncontrolled Search Path Element	11-Nov-2022	7.3	Uncontrolled search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36380**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1369
Unquoted Search Path or Element	11-Nov-2022	7.3	Unquoted search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36384**		
Product: nuc_kit_de3815tykhe					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC Boards, Intel(R) NUC Kits before version TY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-34152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1371
Product: nuc_kit_nuc5i3myhe					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36370		
Insecure Default Initialization of Resource	11-Nov-2022	5.5	Insecure default variable initialization in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2022-36349**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1373
Product: nuc_kit_nuc5i3ryh					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1374
Product: nuc_kit_nuc5i3ryhs					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before	https://www.intel.com/content/www/us/en/security-center/adviso	H-INT-NUC_-221122/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	ry/intel-sa-00752.html	
Product: nuc_kit_nuc5i3ryhsn					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1376
Product: nuc_kit_nuc5i3ryk					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nuc_kit_nuc5i5ryh					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1378
Product: nuc_kit_nuc5i5ryhs					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1379
Product: nuc_kit_nuc5i5ryk					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an	https://www.intel.com/content/www/us/en/security-center/adviso	H-INT-NUC_-221122/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	ry/intel-sa-00752.html	
Product: nuc_kit_nuc5i7ryh					
Affected Version(s): -					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1381
Product: nuc_kit_nuc5pgyh					
Affected Version(s): -					
Incorrect Default Permissions	11-Nov-2022	7.8	Incorrect default permissions in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36377**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Nov-2022	7.8	Path traversal in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36400**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1383
Uncontrolled Search Path Element	11-Nov-2022	7.3	Uncontrolled search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36380**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1384
Unquoted Search Path or Element	11-Nov-2022	7.3	Unquoted search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2022-36384**		
Product: nuc_kit_nuc5ppyh					
Affected Version(s): -					
Incorrect Default Permissions	11-Nov-2022	7.8	Incorrect default permissions in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36377**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1386
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Nov-2022	7.8	Path traversal in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36400**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1387
Uncontrolled Search	11-Nov-2022	7.3	Uncontrolled search path in the	https://www.intel.com/cont	H-INT-NUC_-221122/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path Element			installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36380**	ent/www/us/en/security-center/advisory/intel-sa-00747.html	
Unquoted Search Path or Element	11-Nov-2022	7.3	Unquoted search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36384**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1389
Product: nuc_kit_nuc6cayh					
Affected Version(s): -					
Incorrect Default Permissions	11-Nov-2022	7.8	Incorrect default permissions in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36377**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Nov-2022	7.8	Path traversal in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36400**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1391
Uncontrolled Search Path Element	11-Nov-2022	7.3	Uncontrolled search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36380**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1392
Unquoted Search Path or Element	11-Nov-2022	7.3	Unquoted search path in the installer software for some Intel(r) NUC Kit	https://www.intel.com/content/www/us/en/security-	H-INT-NUC_-221122/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36384**	center/advisory/intel-sa-00747.html	
Product: nuc_kit_nuc6cays					
Affected Version(s): -					
Incorrect Default Permissions	11-Nov-2022	7.8	Incorrect default permissions in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36377**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1394
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Nov-2022	7.8	Path traversal in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2022-36400**		
Uncontrolled Search Path Element	11-Nov-2022	7.3	Uncontrolled search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36380**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1396
Unquoted Search Path or Element	11-Nov-2022	7.3	Unquoted search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36384**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	H-INT-NUC_-221122/1397
Product: nuc_m15_laptop_kit_lapbc510					
Affected Version(s): -					
Improper Restriction of	11-Nov-2022	6.7	Improper buffer restrictions in BIOS firmware for some	https://www.intel.com/content/www/us/	H-INT-NUC_-221122/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Intel(R) NUC M15 Laptop Kits before version BCTGL357.0074 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-32569**	en/security-center/advisory/intel-sa-00752.html	
Product: nuc_m15_laptop_kit_lapbc710					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Nov-2022	6.7	Improper buffer restrictions in BIOS firmware for some Intel(R) NUC M15 Laptop Kits before version BCTGL357.0074 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-32569**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	H-INT-NUC_-221122/1399
Product: xmm_7560					
Affected Version(s): m.2					
Out-of-bounds Write	11-Nov-2022	9.6	Out-of-bounds write in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow an unauthenticated user to potentially	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	H-INT-XMM_-221122/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via adjacent access. **CVE ID : CVE-2022-26513**		
N/A	11-Nov-2022	8.4	Incomplete cleanup in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2022-27639**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	H-INT-XMM_-221122/1401
Improper Check for Unusual or Exceptional Conditions	11-Nov-2022	8.2	Improper conditions check in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-26079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	H-INT-XMM_-221122/1402
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Nov-2022	8.2	Improper buffer restrictions in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	H-INT-XMM_-221122/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-26367**		
Improper Input Validation	11-Nov-2022	8.2	Improper input validation in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-28126**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	H-INT-XMM_-221122/1404
Out-of-bounds Read	11-Nov-2022	8.1	Out-of-bounds read in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2022-26369**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	H-INT-XMM_-221122/1405
Improper Restriction of Operations within the Bounds of	11-Nov-2022	7.2	Improper buffer restrictions in some Intel(R) XMM(TM) 7560 Modem software before version	https://www.intel.com/content/www/us/en/security-center/adviso	H-INT-XMM_-221122/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2022-26045**	ry/intel-sa-00683.html	
Improper Authentication	11-Nov-2022	7.2	Improper authentication in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2022-27874**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	H-INT-XMM_-221122/1407
Improper Input Validation	11-Nov-2022	7.2	Improper input validation in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2022-28611**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	H-INT-XMM_-221122/1408
Vendor: mediatek					
Product: m6789					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310571; Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-M678-221122/1409
Product: mt2731					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT27-221122/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26446		
Product: mt2735					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT27-221122/1411
Product: mt6297					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT62-221122/1412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: mt6580					
Affected Version(s): -					
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT65-221122/1413
Product: mt6725					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: mt6739					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1415
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1417
Product: mt6761					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass due to a parcel format mismatch. This could lead to	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1419
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1420

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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Product: mt6762					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1421
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1423
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. 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/November-2022	H-MED-MT67-221122/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1425
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1426
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT67-221122/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	security-bulletin/November-2022	
Product: mt6762d					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1428
Product: mt6762m					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1429
Product: mt6763					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32601		
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1431
Product: mt6765					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1433
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Product: mt6765t					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1435
Product: mt6767					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: mt6768					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1437
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1439
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1441
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1443
Product: mt6769					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1444
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT67-221122/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	bulletin/November-2022	
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1446
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT67-221122/1447

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: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1448
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**		
Product: mt6769t					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1450
Product: mt6769z					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: mt6771					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1452
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1454
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Product: mt6779					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1456
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1458
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1460
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1461
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race	https://corp.mediatek.com/product-	H-MED-MT67-221122/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	security-bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1463
Product: mt6781					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass due to a parcel format mismatch. This could lead to local escalation of privilege with no additional	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1465
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1467
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1469
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1470
Product: mt6783					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: mt6785					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1472
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT67-221122/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	bulletin/November-2022	
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1474
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-221122/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1476
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1478
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1479
Product: mt6785t					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1480
Product: mt6789					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32601		
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1482
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262364;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07262364. **CVE ID : CVE-2022-32617**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1484
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1485
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race	https://corp.mediatek.com/product-	H-MED-MT67-221122/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	security-bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT67-221122/1487
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. 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/November-2022	H-MED-MT67-221122/1488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**		
Product: mt6833					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1489
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262454; Issue ID: ALPS07262454. **CVE ID : CVE-2022-32618**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1491
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1493
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1494
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1496
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**		
Product: mt6853					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1498
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1500
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1502
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1503
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1505
Product: mt6853t					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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/November-2022	H-MED-MT68-221122/1506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1507
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1509
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1510
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1512
Product: mt6855					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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/November-2022	H-MED-MT68-221122/1513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1514
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262364; Issue ID: ALPS07262364. **CVE ID : CVE-2022-32617**		
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310571; Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1516
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1518
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1519
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	bulletin/November-2022	
Product: mt6873					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1521
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262454; Issue ID: ALPS07262454. **CVE ID : CVE-2022-32618**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1523
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure due to an incorrect bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	bulletin/November-2022	
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1525
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. 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/November-2022	H-MED-MT68-221122/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1527
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1528
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT68-221122/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	security-bulletin/November-2022	
Product: mt6875					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1530
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1532
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1534
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1536
Product: mt6877					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1537
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	bulletin/November-2022	
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1539
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1541
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1543
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1544
Product: mt6879					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1545
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Nov-2022	6.7	In gpu drm, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310704; Issue ID: ALPS07310704. **CVE ID : CVE-2022-32603**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1547
Out-of-bounds Write	08-Nov-2022	6.7	In isp, there is a possible out of bounds write 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. Patch ID: ALPS07213898; Issue ID: ALPS07213898. **CVE ID : CVE-2022-32605**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1548
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1549

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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Out-of-bounds Write	08-Nov-2022	6.7	In isp, 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: ALPS07340373; Issue ID: ALPS07340373. **CVE ID : CVE-2022-32611**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1550
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310571;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1552
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1553
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1555
Product: mt6880					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: mt6883					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1557
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1559
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1561
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1563
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1564
Product: mt6885					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass due to a parcel	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	bulletin/November-2022	
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1566
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure due to an incorrect	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	bulletin/November-2022	
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1568
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. 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/November-2022	H-MED-MT68-221122/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1570
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1572
Product: mt6889					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1573
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	bulletin/November-2022	
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1575
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1576

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: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1577
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1579
Product: mt6890					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: mt6891					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1581
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1583
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32607		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1585
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1586
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1587

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: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1588
Product: mt6893					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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/November-2022	H-MED-MT68-221122/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1590
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262454; Issue ID: ALPS07262454. **CVE ID : CVE-2022-32618**		
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1592
Improper Input Validation	08-Nov-2022	6.7	In gpu drm, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310704;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07310704. **CVE ID : CVE-2022-32603**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1594
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310571; Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1595
Time-of-check Time-of-	08-Nov-2022	6.4	In jpeg, there is a possible use after free due to a race	https://corp.mediatek.com/product-	H-MED-MT68-221122/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388753; Issue ID: ALPS07388753. **CVE ID : CVE-2022-32608**	security-bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1597
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. 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/November-2022	H-MED-MT68-221122/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1599
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1600
Product: mt6895					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1601
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262364; Issue ID: ALPS07262364. **CVE ID : CVE-2022-32617**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1603
Improper Input Validation	08-Nov-2022	6.7	In gpu drm, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310704; Issue ID: ALPS07310704. **CVE ID : CVE-2022-32603**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Nov-2022	6.7	In isp, there is a possible out of bounds write 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. Patch ID: ALPS07213898; Issue ID: ALPS07213898. **CVE ID : CVE-2022-32605**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1605
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1606
Out-of-bounds Write	08-Nov-2022	6.7	In isp, 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/November-2022	H-MED-MT68-221122/1607

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: ALPS07340373; Issue ID: ALPS07340373. **CVE ID : CVE-2022-32611**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Nov-2022	6.4	In jpeg, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388753; Issue ID: ALPS07388753. **CVE ID : CVE-2022-32608**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1608
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1610
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT68-221122/1611
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This	https://corp.mediatek.com/product-security-	H-MED-MT68-221122/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	bulletin/November-2022	
Product: mt6983					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1613
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262364; Issue ID: ALPS07262364. **CVE ID : CVE-2022-32617**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1615
Out-of-bounds Write	08-Nov-2022	6.7	In isp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT69-221122/1616

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: ALPS07213898; Issue ID: ALPS07213898. **CVE ID : CVE-2022-32605**	bulletin/November-2022	
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1617
Out-of-bounds Write	08-Nov-2022	6.7	In isp, 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	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07340373; Issue ID: ALPS07340373. **CVE ID : CVE-2022-32611**		
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310571; Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1619
Improper Input Validation	08-Nov-2022	6.7	In ccd, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326559; Issue ID: ALPS07326559. **CVE ID : CVE-2022-32615**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Nov-2022	6.7	In isp, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07341258; Issue ID: ALPS07341258. **CVE ID : CVE-2022-32616**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1621
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1622
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1624
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32613		
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1626
Product: mt6985					
Affected Version(s): -					
Improper Input Validation	08-Nov-2022	6.7	In gpu drm, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310704; Issue ID: ALPS07310704. **CVE ID : CVE-2022-32603**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT69-221122/1627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8167					
Affected Version(s): -					
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1628
Product: mt8167s					
Affected Version(s): -					
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1629
Product: mt8168					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1630
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1631
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This	https://corp.mediatek.com/product-security-	H-MED-MT81-221122/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310571; Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1633
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1635
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1636
Product: mt8173					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1637
Product: mt8175					
Affected Version(s): -					
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1638
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a	https://corp.mediatek.com/product-	H-MED-MT81-221122/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	security-bulletin/November-2022	
Product: mt8183					
Affected Version(s): -					
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1640
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1641

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. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**		
Product: mt8185					
Affected Version(s): -					
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1642
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1644
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT81-221122/1646
Product: mt8321					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1648
Product: mt8362a					
Affected Version(s): -					
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1649
Product: mt8365					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1650
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1651
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT83-221122/1652

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: ALPS07310571; Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1653
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1655
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1656
Product: mt8385					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1657
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1659
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT83-221122/1660
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT83-221122/1661

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. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	bulletin/November-2022	
Product: mt8666					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1662
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1664
Product: mt8667					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: mt8675					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1666
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This	https://corp.mediatek.com/product-security-	H-MED-MT86-221122/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	bulletin/November-2022	
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1668
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**		
Product: mt8696					
Affected Version(s): -					
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1670
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1672
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT86-221122/1674
Product: mt8765					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1675
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT87-221122/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	bulletin/November-2022	
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1677
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT87-221122/1678

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. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	bulletin/November-2022	
Product: mt8766					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1679
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1681
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**		
Product: mt8768					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1683
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1685
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1687
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1688
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This	https://corp.mediatek.com/product-security-	H-MED-MT87-221122/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	bulletin/November-2022	
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1690
Product: mt8786					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass due to a parcel format mismatch. This could lead to local escalation of privilege with no	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1692
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1694
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32610		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1696
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1697
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1698

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. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**		
Product: mt8788					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1699
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1701
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Product: mt8789					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1703
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1705
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1707
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1708
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-221122/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	bulletin/November-2022	
Product: mt8791					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1710
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after	https://corp.mediatek.com	H-MED-MT87-221122/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	/product-security-bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1712
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1714
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1716
Product: mt8791t					
Affected Version(s): -					
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1717
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to	https://corp.mediatek.com/product-	H-MED-MT87-221122/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	security-bulletin/November-2022	
Product: mt8795t					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1719
Improper Input Validation	08-Nov-2022	6.7	In gpu drm, there is a possible out of bounds write due to improper input validation. This	https://corp.mediatek.com/product-security-	H-MED-MT87-221122/1720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310704; Issue ID: ALPS07310704. **CVE ID : CVE-2022-32603**	bulletin/November-2022	
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1721
Product: mt8797					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass due to a parcel format mismatch. This could lead to local escalation of privilege with no additional	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1723
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310571; Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1725
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1727
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1728
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**		
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1730
Product: mt8798					
Affected Version(s): -					
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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/November-2022	H-MED-MT87-221122/1731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262364; Issue ID: ALPS07262364. **CVE ID : CVE-2022-32617**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1732
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07262454; Issue ID: ALPS07262454. **CVE ID : CVE-2022-32618**		
Improper Input Validation	08-Nov-2022	6.7	In gpu drm, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310704; Issue ID: ALPS07310704. **CVE ID : CVE-2022-32603**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1734
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310571; Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1736
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1737
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT87-221122/1739
Product: mt8871					
Affected Version(s): -					
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891;	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT88-221122/1740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Improper Input Validation	08-Nov-2022	6.7	In ccd, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326559; Issue ID: ALPS07326559. **CVE ID : CVE-2022-32615**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT88-221122/1741
Improper Input Validation	08-Nov-2022	6.7	In isp, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07341258; Issue ID: ALPS07341258. **CVE ID : CVE-2022-32616**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT88-221122/1742
Product: mt8891					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT88-221122/1743
Improper Input Validation	08-Nov-2022	6.7	In ccd, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326559; Issue ID: ALPS07326559. **CVE ID : CVE-2022-32615**	https://corp.mediatek.com/product-security-bulletin/November-2022	H-MED-MT88-221122/1744
Improper Input Validation	08-Nov-2022	6.7	In isp, there is a possible out of bounds write due to uninitialized data. This could	https://corp.mediatek.com/product-security-	H-MED-MT88-221122/1745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07341258; Issue ID: ALPS07341258. **CVE ID : CVE-2022-32616**	bulletin/November-2022	
Vendor: mitshubishielectric					
Product: mac-507if-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mac-587if-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-587if2-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-588if-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-002if					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-S-MA-221122/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Vendor: Mitsubishielectric					
Product: ma-ew85s-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MA-E-221122/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MA-E-221122/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: ma-ew85s-uk					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MA-E-221122/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MA-E-221122/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33322**		
Product: mac-507if-e					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MAC--221122/1755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mac-557if-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-557if-e1					
Affected Version(s): -					
Cleartext Transmission of	08-Nov-2022	9.8	Cleartext Transmission of Sensitive	https://www.mitsubishielectric.com/en/p	H-MIT-MAC--221122/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing	sirt/vulnerability/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-558if-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-558if-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-559if-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-559if-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: mac-566ifb-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-567ifb-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-567ifb2-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-568if-e					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-568ifb-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-568ifb2-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-568ifb3-e					
Affected Version(s): -					
Cleartext Transmission of	08-Nov-2022	9.8	Cleartext Transmission of Sensitive	https://www.mitsubishielectric.com/en/p	H-MIT-MAC--221122/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing	sirt/vulnerability/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-576if-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MAC--221122/1769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-587if-e					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MAC--221122/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mac-587if2-e					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MAC--221122/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mac-588if-e					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MAC--221122/1772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mfz-gxt50\/60\/73vfk					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MFZ--221122/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MFZ--221122/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mfz-xt50\/60vfk					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MFZ--221122/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/p	H-MIT-MFZ--221122/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	sirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msxy-fp05\/07\/10\/13\/18\/20\/24vgk-sg1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSXY-221122/1777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSXY-221122/1778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msy-gp10\/13\/15\/18\/20\/24vfk-sg1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSY--221122/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSY--221122/1780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-e2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-er2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-et2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap22\/25\/35\/42\/50\/60\/71\/80vgkd-a2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap22\/25\/35\/42\/50\/61\/70\/80vgkd-a1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-e6					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ap25\/35\/42\/50vgk-e7					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-e8					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-en1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-en2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-en3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50\/60\/71vgk-e3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50\/60\/71vgk-er3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ap25\/35\/42\/50\/60\/71vgk-et3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap60\/71vgk-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ap60\/71vgk-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: msz-ap60\/71vgk-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ay25\/35\/42\/50vgk-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgk-e6					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgk-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgk-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgk-sc1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgkp-e6					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ay25\/35\/42\/50vgkp-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgkp-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgkp-sc1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-bt20\/25\/35\/50vgk-e2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-e3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-er2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-et2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-et3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/1850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ef18\/22\/25\/35\/42\/50vgkb-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef18\/22\/25\/35\/42\/50vgkb-e2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef18\/22\/25\/35\/42\/50vgks-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef18\/22\/25\/35\/42\/50vgks-e2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-ef18\/22\/25\/35\/42\/50vgkw-e1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef18\/22\/25\/35\/42\/50vgkw-e2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-a1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-er2					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-et2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/1872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ef22\/25\/35\/42\/50vgks-a1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgks-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgks-er2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgks-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-ef22\/25\/35\/42\/50vgks-et2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-a1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-er2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-et2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-exa09\/12vak					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-eza09\/12vak					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft20\/25vfk					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ft25\/35\/50vgk-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft25\/35\/50vgk-e2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft25\/35\/50vgk-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft25\/35\/50vgk-sc1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft25\/35\/50vgk-sc2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/1907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-fx20\/25vfk					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-gzt09\/12\/18vak					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-gzy09\/12\/18vfk					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33322**		
Product: msz-hr25\/35\/42\/50vfk-e6					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-hr25\/35\/42\/50\/60\/71vfk-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-hr25\/35\/42\/50\/60\/71vfk-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-hr25\/35\/42\/50\/60\/71vfk-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/p	H-MIT-MSZ--221122/1919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	sirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ky09\/12\/18vfk					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50vg2b-en1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50vg2r-en1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: msz-ln18\/25\/35\/50vg2v-en1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50vg2w-en1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50vg2w-sc1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2b-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2b-e2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2b-e3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2b-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2r-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2r-e2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2r-e3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2r-et1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2v-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2v-e2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2v-e3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2v-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2w-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2w-e2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2w-e3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2w-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: msz-ln18\/25\/35\/50\/60vg2w-er2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2w-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2w-et2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vgb-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vgr-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vgv-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: msz-ln18\/25\/35\/50\/60vgw-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50vg2b-en2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2b-sc1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2r-en2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2r-sc1					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2v-en2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2v-sc1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ln25\/35\/50vg2w-en2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-a1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2b-a2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2b-er2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-er3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-et2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-et3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2r-a1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2r-a2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ln25\/35\/50\/60vg2r-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2r-er2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2r-er3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2r-et2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2r-et3					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/1998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2v-a1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/1999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2v-a2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2v-er1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2v-er2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2v-er3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/2006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ln25\/35\/50\/60vg2v-et2					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2v-et3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2w-er3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2w-et3					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/2014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-ln25\/35\/50\/60vgb-a1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgb-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgr-a1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgr-er1					
Affected Version(s): -					
Cleartext Transmissi on of	08-Nov-2022	9.8	Cleartext Transmission of Sensitive	https://www.mitsubishielectric.com/en/p	H-MIT-MSZ--221122/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing	sirt/vulnerability/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgv-a1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgv-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgw-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-rw25\/35\/50vg-e1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-rw25\/35\/50vg-er1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-rw25\/35\/50vg-et1					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-MSZ--221122/2026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-rw25\/35\/50vg-sc1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-wx18\/20\/25vfk					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	H-MIT-MSZ--221122/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-zt09\/12\/18vak					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-zy09\/12\/18vfk					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-MSZ--221122/2033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-MSZ--221122/2034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: pac-wf010-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-PAC--221122/2035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: pac-whs01wf-e					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-PAC--221122/2036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-002if					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	H-MIT-S-MA-221122/2037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: s-mac-702if-b					
Affected Version(s): -					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-S-MA-221122/2038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-702if-f					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-S-MA-221122/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-702if-z					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-S-MA-221122/2040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-905if					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-S-MA-221122/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-906if					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	H-MIT-S-MA-221122/2042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Vendor: Phoenixcontact					
Product: fl_mguard_centerport					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2043
Product: fl_mguard_centerport_vpn-1000					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated	N/A	H-PHO-FL_M-221122/2044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_core_tx					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2045
Product: fl_mguard_core_tx_vpn					
Affected Version(s): -					
Allocation of Resources Without	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX	N/A	H-PHO-FL_M-221122/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_delta_tx\/tx					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2047
Product: fl_mguard_delta_tx\/tx_vpn					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2048
Product: fl_mguard_gt\/gt					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for	N/A	H-PHO-FL_M-221122/2049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_gt\/gt_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2050
Product: fl_mguard_pci4000					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger	N/A	H-PHO-FL_M-221122/2051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_pci4000_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2052
Product: fl_mguard_pcie4000					
Affected Version(s): -					
Allocation of Resources	15-Nov-2022	7.5	A remote, unauthenticated attacker could	N/A	H-PHO-FL_M-221122/2053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_pcie4000_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue.	N/A	H-PHO-FL_M-221122/2054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3480		
Product: fl_mguard_rs2000_tx\/tx-b					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2055
Product: fl_mguard_rs2000_tx\/tx_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from	N/A	H-PHO-FL_M-221122/2056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_rs2005_tx_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2057
Product: fl_mguard_rs4000_tx\/tx					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC	N/A	H-PHO-FL_M-221122/2058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_rs4000_tx\/tx-m					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2059
Product: fl_mguard_rs4000_tx\/tx-p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2060
Product: fl_mguard_rs4000_tx\/tx_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming	N/A	H-PHO-FL_M-221122/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_rs4004_tx\/dtx					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2062
Product: fl_mguard_rs4004_tx\/dtx_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of	N/A	H-PHO-FL_M-221122/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_smart2					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-FL_M-221122/2064
Product: fl_mguard_smart2_vpn					
Affected Version(s): -					
Allocation of Resources Without	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-	N/A	H-PHO-FL_M-221122/2065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: tc_mguard_rs2000_3g_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-TC_M-221122/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tc_mguard_rs2000_4g_att_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-TC_M-221122/2067
Product: tc_mguard_rs2000_4g_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring	N/A	H-PHO-TC_M-221122/2068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: tc_mguard_rs2000_4g_vzw_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-TC_M-221122/2069
Product: tc_mguard_rs4000_3g_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0	N/A	H-PHO-TC_M-221122/2070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: tc_mguard_rs4000_4g_att_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	H-PHO-TC_M-221122/2071
Product: tc_mguard_rs4000_4g_vpn					
Affected Version(s): -					
Allocation of	15-Nov-2022	7.5	A remote, unauthenticated	N/A	H-PHO-TC_M-221122/2072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: tc_mguard_rs4000_4g_vzw_vpn					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue.	N/A	H-PHO-TC_M-221122/2073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3480		
Vendor: Samsung					
Product: exynos					
Affected Version(s): -					
Out-of-bounds Read	09-Nov-2022	9.1	Improper input validation vulnerability for processing SIB12 PDU in Exynos modems prior to SMR Sep-2022 Release allows remote attacker to read out of bounds memory. **CVE ID : CVE-2022-39881**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	H-SAM-EXYN-221122/2074
Vendor: sick					
Product: sim1000_fx					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality	https://sick.com/psirt	H-SIC-SIM1-221122/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SIM1000 FX Partnumber 1097816 and 1097817 with firmware version < 1.6.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. The recommended solution is to update the	https://sick.com/psirt	H-SIC-SIM1-221122/2076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware to a version >= 1.6.0 as soon as possible. (available in SICK Support Portal) **CVE ID : CVE-2022-27585**		
Product: sim1004					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general	https://sick.com/psirt	H-SIC-SIM1-221122/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Product: sim1004-0p0g311					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SIM1004 Partnumber 1098148 with firmware version < 2.0.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a	https://sick.com/psirt	H-SIC-SIM1-221122/2078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version >= 2.0.0 as soon as possible. **CVE ID : CVE-2022-27586**		
Product: sim1012					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security	https://sick.com/psirt	H-SIC-SIM1-221122/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Product: sim1012-0p0g200					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	7.3	Password recovery vulnerability in SICK SIM1012 Partnumber 1098146 with firmware version < 2.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. The recommended solution is to update the firmware to a version >= 2.2.0 as soon as possible. (available in SICK Support Portal) **CVE ID : CVE-2022-43990**	https://sick.com/psirt	H-SIC-SIM1-221122/2080
Product: sim2000					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an	https://sick.com/psirt	H-SIC-SIM2-221122/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Product: sim2000-2p04g10					
Affected Version(s): -					
Missing Authentication for	01-Nov-2022	7.3	Password recovery vulnerability in SICK SIM2x00 (ARM) Partnumber	https://sick.com/psirt	H-SIC-SIM2-221122/2082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			1092673 and 1081902 with firmware version <= 1.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. The recommended solution is to update the firmware to a version >1.2.0 as soon as possible. **CVE ID : CVE-2022-43989**		
Product: sim2000st					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting	https://sick.com/psirt	H-SIC-SIM2-221122/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SIM2000ST Partnumber 2086502 and 1080579 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting	https://sick.com/psirt	H-SIC-SIM2-221122/2084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM2000ST. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27584**		
Product: sim2500					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and	https://sick.com/psirt	H-SIC-SIM2-221122/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Product: sim2500-2p03g10					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	7.3	Password recovery vulnerability in SICK SIM2x00 (ARM) Partnumber 1092673 and 1081902 with firmware version <= 1.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism	https://sick.com/psirt	H-SIC-SIM2-221122/2086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method. The recommended solution is to update the firmware to a version >1.2.0 as soon as possible. **CVE ID : CVE-2022-43989**		
Product: sim4000					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the	https://sick.com/psirt	H-SIC-SIM4-221122/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIM4000. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Vendor: Siemens					
Product: 6ag1151-8ab01-7ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6AG1-221122/2088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1151-8fb01-2ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6AG1-221122/2089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1314-6eh04-7ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6AG1-221122/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1315-2eh14-7ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6AG1-221122/2091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1315-2fj14-2ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6AG1-221122/2092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1317-2ek14-7ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6AG1-221122/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1317-2fk14-2ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6AG1-221122/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7151-8ab01-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7151-8fb01-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7154-8ab01-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7154-8fb01-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7154-8fx00-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7314-6eh04-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7315-2eh14-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7315-2fj14-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7315-7tj10-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7317-2ek14-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7317-2fk14-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7317-7tk10-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7317-7ul10-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7318-3el01-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7318-3fl01-0ab0					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-6ES7-221122/2109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 7kg9501-0aa01-2aa1					
Affected Version(s): -					
Session Fixation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not renew the session cookie after login/logout and also accept user defined session cookies. An attacker could overwrite the stored session cookie of a user. After the victim logged in, the attacker is given access to the user's account through the activated session. **CVE ID : CVE-2022-43398**	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	H-SIE-7KG9-221122/2110
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50).	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	H-SIE-7KG9-221122/2111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected devices do not properly validate the Language-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device. **CVE ID : CVE-2022-43439**		
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the RecordType-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	H-SIE-7KG9-221122/2112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on the device. **CVE ID : CVE-2022-43545**		
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the EndTime-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device. **CVE ID : CVE-2022-43546**	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	H-SIE-7KG9-221122/2113
Product: 7kg9501-0aa31-2aa1					
Affected Version(s): -					
Session Fixation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	H-SIE-7KG9-221122/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not renew the session cookie after login/logout and also accept user defined session cookies. An attacker could overwrite the stored session cookie of a user. After the victim logged in, the attacker is given access to the user's account through the activated session. **CVE ID : CVE-2022-43398**		
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the Language-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	H-SIE-7KG9-221122/2115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on the device. **CVE ID : CVE-2022-43439**		
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the RecordType-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device. **CVE ID : CVE-2022-43545**	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	H-SIE-7KG9-221122/2116
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the EndTime-	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	H-SIE-7KG9-221122/2117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device. **CVE ID : CVE-2022-43546**		
Product: simatic_drive_controller_cpu_1504d_tf					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_drive_controller_cpu_1507d_tf					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_pcs					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants)	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1211c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1212c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1212fc					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1214c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1214fc					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1214_fc					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1215c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1215fc					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1215_fc					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1217c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1211c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1212c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1212fc					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1214c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1214fc					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1215c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1215fc					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1217c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1507s					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1507s_f					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1508s					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1508s_f					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1510sp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1510sp-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511-1_pn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511c-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511f-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511f-1_pn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511t-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511tf-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1512c					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1512c-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1512sp-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1512spf-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513-1_pn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513f-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513f-1_pn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513r-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515-2_pn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_151511c-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_151511f-1					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515f-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515f-2_pn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515r-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515t-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515tf-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516-3					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516-3_dp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516-3_pn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516-3_pn\/dp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516f-3					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516f-3_pn\/dp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516pro-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516pro_f					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516t-3					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516tf-3					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517-3					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517-3_dp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517-3_pn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517-3_pn\/dp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517f-3					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517f-3_pn\/dp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517tf-3					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4_dp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4_pn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4_pn\/dp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4_pn\/dp_mfp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518f-4					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518f-4_pn\/dp					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518hf-4					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518t-4					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518tf-4					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_15pro-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_15prof-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_cpu_1513pro-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_cpu_1513prof-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-400_pn\/dp_v6					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-400_pn\/dp_v7					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SIMA-221122/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: sinumerik_one					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	H-SIE-SINU-221122/2205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Vendor: Tenda					
Product: ac23					
Affected Version(s): -					
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the devName parameter in the formSetDeviceName function. **CVE ID : CVE-2022-43101**	N/A	H-TEN-AC23-221122/2206
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the timeZone parameter in the fromSetSysTime function. **CVE ID : CVE-2022-43102**	N/A	H-TEN-AC23-221122/2207
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2022-43103**	N/A	H-TEN-AC23-221122/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the wpapsk_crypto parameter in the fromSetWirelessRepeat function. **CVE ID : CVE-2022-43104**	N/A	H-TEN-AC23-221122/2209
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the shareSpeed parameter in the fromSetWifiGusetBasic function. **CVE ID : CVE-2022-43105**	N/A	H-TEN-AC23-221122/2210
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the schedStartTime parameter in the setSchedWifi function. **CVE ID : CVE-2022-43106**	N/A	H-TEN-AC23-221122/2211
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the time parameter in the setSmartPowerManagement function.	N/A	H-TEN-AC23-221122/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43107		
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the firewallEn parameter in the formSetFirewallCfg function. **CVE ID : CVE-2022-43108**	N/A	H-TEN-AC23-221122/2213
Vendor: westerndigital					
Product: my_cloud_home					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Nov-2022	4.3	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability was discovered via an HTTP API on Western Digital My Cloud Home; My Cloud Home Duo; and SanDisk ibi devices that could allow an attacker to abuse certain parameters to point to random locations on the file system. This could also allow the attacker to initiate the installation of custom packages at these locations. This can only be	https://www.westerndigital.com/support/product-security/wdc-22016-my-cloud-home-ibi-firmware-version-8-11-0-113	H-WES-MY_C-221122/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited once the attacker has been authenticated to the device. This issue affects: Western Digital My Cloud Home and My Cloud Home Duo versions prior to 8.11.0-113 on Linux; SanDisk ibi versions prior to 8.11.0-113 on Linux. **CVE ID : CVE-2022-29836**		
Product: my_cloud_home_duo					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Nov-2022	4.3	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability was discovered via an HTTP API on Western Digital My Cloud Home; My Cloud Home Duo; and SanDisk ibi devices that could allow an attacker to abuse certain parameters to point to random locations on the file system. This could also allow the attacker to initiate the installation of custom packages at these locations.	https://www.westerndigital.com/support/product-security/wdc-22016-my-cloud-home-ibi-firmware-version-8-11-0-113	H-WES-MY_C-221122/2215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This can only be exploited once the attacker has been authenticated to the device. This issue affects: Western Digital My Cloud Home and My Cloud Home Duo versions prior to 8.11.0-113 on Linux; SanDisk ibi versions prior to 8.11.0-113 on Linux. **CVE ID : CVE-2022-29836**		
Product: sandisk_ibi					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Nov-2022	4.3	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability was discovered via an HTTP API on Western Digital My Cloud Home; My Cloud Home Duo; and SanDisk ibi devices that could allow an attacker to abuse certain parameters to point to random locations on the file system. This could also allow the attacker to initiate the installation of custom packages at	https://www.westerndigital.com/support/product-security/wdc-22016-my-cloud-home-ibi-firmware-version-8-11-0-113	H-WES-SAND-221122/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these locations. This can only be exploited once the attacker has been authenticated to the device. This issue affects: Western Digital My Cloud Home and My Cloud Home Duo versions prior to 8.11.0-113 on Linux; SanDisk ibi versions prior to 8.11.0-113 on Linux. **CVE ID : CVE-2022-29836**		
Vendor: wut					
Product: at-modem-emulator					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-AT-M-221122/2217
Improper Neutralization of Input During Web Page	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated	N/A	H-WUT-AT-M-221122/2218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_20ma					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unauthenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2219
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the	N/A	H-WUT-COM--221122/2220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_highspeed_100basefx					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2221
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2222
Product: com-server_highspeed_100baselx					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2223
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2224
Product: com-server_highspeed_19\"_1port					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2226
Product: com-server_highspeed_19\"_4port					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unauthenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2228
Product: com-server_highspeed_compact					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2229
Improper Neutralization of Input During Web Page Generation	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute	N/A	H-WUT-COM--221122/2230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_highspeed_industry					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2231
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage	N/A	H-WUT-COM--221122/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42786		
Product: com-server_highspeed_isolated					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2233
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2234
Product: com-server_highspeed_lc					
Affected Version(s): -					
Use of Insufficient	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series	https://cert.vde.com/de/ad	H-WUT-COM--221122/2235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	visories/VDE-2022-043	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2236
Product: com-server_highspeed_oem					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account on the the device. **CVE ID : CVE-2022-42787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2238
Product: com-server_highspeed_office_1port					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2239
Improper Neutralization of	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series	N/A	H-WUT-COM--221122/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_highspeed_office_4port					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2241
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload	N/A	H-WUT-COM--221122/2242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_highspeed_poe					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2243
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2244
Product: com-server_highspeed_poe_3x_isolated					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2245
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2246
Product: com-server_highspeed_ul					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2248
Product: com-server_\+\+					
Affected Version(s): -					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device.	https://cert.vde.com/de/advisories/VDE-2022-043	H-WUT-COM--221122/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42787		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	H-WUT-COM--221122/2250
Operating System					
Vendor: AMD					
Product: a10-9600p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-A10--221122/2251
Product: a10-9630p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions	https://www.amd.com/en/corporate/pro	O-AMD-A10--221122/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	duct-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: a12-9700p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-A12--221122/2253
Product: a12-9730p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-A12--221122/2254
Product: a4-9120_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-A4-9-221122/2255
Product: a6-9210_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-A6-9-221122/2256
Product: a6-9220c_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-A6-9-221122/2257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: a6-9220_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-A6-9-221122/2258
Product: a9-9410_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-A9-9-221122/2259
Product: a9-9420_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	O-AMD-A9-9-221122/2260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: athlon_gold_3150u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2261
Product: athlon_silver_3050u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2262
Product: athlon_x4_750_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	O-AMD-ATHL-221122/2263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: athlon_x4_760k_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2264
Product: athlon_x4_830_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2265
Product: athlon_x4_835_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	O-AMD-ATHL-221122/2266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: athlon_x4_840_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2267
Product: athlon_x4_845_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2268
Product: athlon_x4_860k_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	O-AMD-ATHL-221122/2269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: athlon_x4_870k_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2270
Product: athlon_x4_880k_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2271
Product: athlon_x4_940_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	O-AMD-ATHL-221122/2272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: athlon_x4_950_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2273
Product: athlon_x4_970_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-ATHL-221122/2274
Product: epyc_7001_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2275
Product: epyc_7002_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2276
Product: epyc_7003_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: epyc_7251_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2278
Product: epyc_7252_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2279
Product: epyc_7261_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	O-AMD-EPYC-221122/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: epyc_7262_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2281
Product: epyc_7272_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2282
Product: epyc_7281_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	O-AMD-EPYC-221122/2283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7282_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2284
Product: epyc_72f3_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2285
Product: epyc_7301_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	O-AMD-EPYC-221122/2286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7302p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2287
Product: epyc_7302_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2288
Product: epyc_7313p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-221122/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7313_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2290
Product: epyc_7343_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2291
Product: epyc_7351p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	O-AMD-EPYC-221122/2292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7351_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2293
Product: epyc_7352_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2294
Product: epyc_7371_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2295
Product: epyc_7373x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2296
Product: epyc_7401p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: epyc_7401_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2298
Product: epyc_7402p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2299
Product: epyc_7402_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	O-AMD-EPYC-221122/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: epyc_7413_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2301
Product: epyc_7443p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2302
Product: epyc_7443_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	O-AMD-EPYC-221122/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7451_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2304
Product: epyc_7452_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2305
Product: epyc_7473x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	O-AMD-EPYC-221122/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_74f3_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2307
Product: epyc_7501_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2308
Product: epyc_7502p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-221122/2309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7502_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2310
Product: epyc_7513_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2311
Product: epyc_7532_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	O-AMD-EPYC-221122/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7542_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2313
Product: epyc_7543p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2314
Product: epyc_7543_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2315
Product: epyc_7551p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2316
Product: epyc_7551_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: epyc_7552_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2318
Product: epyc_7573x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2319
Product: epyc_75f3_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	O-AMD-EPYC-221122/2320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: epyc_7601_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2321
Product: epyc_7642_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2322
Product: epyc_7643_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	O-AMD-EPYC-221122/2323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7662_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2324
Product: epyc_7663_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2325
Product: epyc_7702_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	O-AMD-EPYC-221122/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7713p_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2327
Product: epyc_7713_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2328
Product: epyc_7742_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	O-AMD-EPYC-221122/2329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7763_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2330
Product: epyc_7773x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2331
Product: epyc_7f32_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	O-AMD-EPYC-221122/2332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: epyc_7f52_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2333
Product: epyc_7f72_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2334
Product: epyc_7h12_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-EPYC-221122/2335
Product: ryzen_3_2200u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2336
Product: ryzen_3_2300u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ryzen_3_3100_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2338
Product: ryzen_3_3200u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2339
Product: ryzen_3_3250u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	O-AMD-RYZE-221122/2340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: ryzen_3_3300g_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2341
Product: ryzen_3_3300u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2342
Product: ryzen_3_3300x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	O-AMD-RYZE-221122/2343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_3_4300ge_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2344
Product: ryzen_3_4300g_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2345
Product: ryzen_3_4300u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	O-AMD-RYZE-221122/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_3_5125c_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2347
Product: ryzen_3_5400u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2348
Product: ryzen_3_5425c_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	O-AMD-RYZE-221122/2349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_3_5425u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2350
Product: ryzen_5_2500u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2351
Product: ryzen_5_2600h_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	O-AMD-RYZE-221122/2352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_2600x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2353
Product: ryzen_5_2600_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2354
Product: ryzen_5_2700x_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2355
Product: ryzen_5_2700_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2356
Product: ryzen_5_3400g_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ryzen_5_3450g_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2358
Product: ryzen_5_3500u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2359
Product: ryzen_5_3550h_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	O-AMD-RYZE-221122/2360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: ryzen_5_3580u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2361
Product: ryzen_5_3600xt_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2362
Product: ryzen_5_3600x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	O-AMD-RYZE-221122/2363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_3600_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2364
Product: ryzen_5_4500u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2365
Product: ryzen_5_4600ge_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	O-AMD-RYZE-221122/2366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_4600g_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2367
Product: ryzen_5_4600h_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2368
Product: ryzen_5_4600u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	O-AMD-RYZE-221122/2369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_5560u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2370
Product: ryzen_5_5600hs_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2371
Product: ryzen_5_5600h_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	O-AMD-RYZE-221122/2372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_5_5600u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2373
Product: ryzen_5_5625c_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2374
Product: ryzen_5_5625u_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2375
Product: ryzen_7_2700u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2376
Product: ryzen_7_2700x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ryzen_7_2700_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2378
Product: ryzen_7_2800h_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2379
Product: ryzen_7_3700u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	O-AMD-RYZE-221122/2380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: ryzen_7_3700x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2381
Product: ryzen_7_3750h_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2382
Product: ryzen_7_3780u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	O-AMD-RYZE-221122/2383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_7_3800xt_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2384
Product: ryzen_7_3800x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2385
Product: ryzen_7_4700ge_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	O-AMD-RYZE-221122/2386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_7_4700g_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2387
Product: ryzen_7_4700u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2388
Product: ryzen_7_4800h_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	O-AMD-RYZE-221122/2389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_7_4800u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2390
Product: ryzen_7_5800hs_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2391
Product: ryzen_7_5800h_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	O-AMD-RYZE-221122/2392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_7_5800u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2393
Product: ryzen_7_5825c_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2394
Product: ryzen_7_5825u_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2395
Product: ryzen_7_pro_3700u_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2396
Product: ryzen_9_4900h_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ryzen_9_5900hs_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2398
Product: ryzen_9_5900hx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2399
Product: ryzen_9_5980hs_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-	O-AMD-RYZE-221122/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23824	security/2022/11/10/2	
Product: ryzen_9_5980hx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2401
Product: ryzen_threadripper_2920x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2402
Product: ryzen_threadripper_2950x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.o	O-AMD-RYZE-221122/2403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	penwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_threadripper_2970wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2404
Product: ryzen_threadripper_2990wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2405
Product: ryzen_threadripper_3960x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-	O-AMD-RYZE-221122/2406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_threadripper_3970x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2407
Product: ryzen_threadripper_3990x_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2408
Product: ryzen_threadripper_pro_3795wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being	https://www.amd.com/en/corporate/product-	O-AMD-RYZE-221122/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_threadripper_pro_3945wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2410
Product: ryzen_threadripper_pro_3955wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2411
Product: ryzen_threadripper_pro_3995wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return	https://www.amd.com/en/	O-AMD-RYZE-221122/2412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	
Product: ryzen_threadripper_pro_5945wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2413
Product: ryzen_threadripper_pro_5955wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2414
Product: ryzen_threadripper_pro_5965wx_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2415
Product: ryzen_threadripper_pro_5975wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2416
Product: ryzen_threadripper_pro_5995wx_firmware					
Affected Version(s): -					
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure. **CVE ID : CVE-2022-23824**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/lists/oss-security/2022/11/10/2	O-AMD-RYZE-221122/2417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 15.5					
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26709**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-IPAD-221122/2418
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, tvOS 15.5, watchOS 8.6. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://suppo	O-APP-IPAD-221122/2419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26710	rt.apple.com/en-us/HT213258	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26716**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-IPAD-221122/2420
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5, iTunes 12.12.4 for Windows. Processing maliciously crafted web content may	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://suppo	O-APP-IPAD-221122/2421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2022-26717**	rt.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258, https://support.apple.com/en-us/HT213259	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26719**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-IPAD-221122/2422
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS	https://support.apple.com/en-us/HT213257, https://suppo	O-APP-IPAD-221122/2423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Monterey 12.4, iOS 15.5 and iPadOS 15.5. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2022-26762**	rt.apple.com/en-us/HT213258	
N/A	01-Nov-2022	4.3	A logic issue in the handling of concurrent media was addressed with improved state handling. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. Video self-preview in a webRTC call may be interrupted if the user answers a phone call. **CVE ID : CVE-2022-22677**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213258	O-APP-IPAD-221122/2424
Affected Version(s): * Up to (excluding) 15.7					
N/A	01-Nov-2022	7.8	This issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.7 and iPadOS 15.7, macOS Ventura 13. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-42796**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213445	O-APP-IPAD-221122/2425
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state	https://support.apple.com/en-	O-APP-IPAD-221122/2426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. A user may be able to view restricted content from the lock screen. **CVE ID : CVE-2022-42790**	us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	
Improper Input Validation	01-Nov-2022	5.5	An issue in code signature validation was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. An app may be able to bypass code signing checks. **CVE ID : CVE-2022-42793**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213445, https://support.apple.com/	O-APP-IPAD-221122/2427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213446	
N/A	01-Nov-2022	2.4	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, tvOS 16. A user with physical access to a device may be able to access contacts from the lock screen. **CVE ID : CVE-2022-32879**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-221122/2428
Affected Version(s): * Up to (excluding) 15.7.1					
N/A	01-Nov-2022	7.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A user may be able to cause unexpected app termination or	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213493, https://suppo	O-APP-IPAD-221122/2429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2022-42800**	rt.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
Out-of-bounds Write	01-Nov-2022	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-42827**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2430
Concurrent Execution using Shared Resource with Improper Synchronization	01-Nov-2022	7	A race condition was addressed with improved locking. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16,	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494,	O-APP-IPAD-221122/2431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42803**	https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS 9.1. Visiting a maliciously crafted website may leak sensitive data. **CVE ID : CVE-2022-42817**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2432
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16,	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494,	O-APP-IPAD-221122/2433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.6.1, macOS Big Sur 11.7.1. Parsing a maliciously crafted audio file may lead to disclosure of user information. **CVE ID : CVE-2022-42798**	https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491	
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing a maliciously crafted USD file may disclose memory contents. **CVE ID : CVE-2022-42810**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2434
Affected Version(s): * Up to (excluding) 16.0					
Out-of-bounds Write	01-Nov-2022	9.8	An out-of-bounds write issue was addressed with improved bounds	https://support.apple.com/en-us/HT213488	O-APP-IPAD-221122/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-42808**	, https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	
Improper Certificate Validation	01-Nov-2022	9.8	A certificate validation issue existed in the handling of WKWebView. This issue was addressed with improved validation. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. Processing a maliciously crafted certificate may lead to arbitrary code execution. **CVE ID : CVE-2022-42813**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2436
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS	https://support.apple.com/en-us/HT213488 , https://support.apple.com/	O-APP-IPAD-221122/2437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-42823**	en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app may cause unexpected app termination or arbitrary code execution. **CVE ID : CVE-2022-42820**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2438
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	7	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42806		
Improper Restriction of Rendered UI Layers or Frames	01-Nov-2022	6.1	The issue was addressed with improved UI handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Visiting a malicious website may lead to user interface spoofing. **CVE ID : CVE-2022-42799**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2440
N/A	01-Nov-2022	5.5	An access issue was addressed with additional sandbox restrictions. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-42811**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/	O-APP-IPAD-221122/2441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213489	
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state management. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose sensitive user information. **CVE ID : CVE-2022-42824**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2442
N/A	01-Nov-2022	5.5	This issue was addressed by removing additional entitlements. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to modify protected parts of the file system.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/	O-APP-IPAD-221122/2443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42825	en-us/HT213493, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
Affected Version(s): * Up to (excluding) 5.7.1					
N/A	01-Nov-2022	7.8	A logic issue was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42801**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2444
Product: ipad_os					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 15.7					
Out-of-bounds Write	01-Nov-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, macOS Monterey 12.6, tvOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32888**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445	O-APP-IPAD-221122/2445
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-	O-APP-IPAD-221122/2446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32898	us/HT213445, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32899**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-221122/2447
N/A	01-Nov-2022	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 15.7 and iPadOS 15.7, iOS 16.1 and iPadOS 16. An app may be able to access iOS backups. **CVE ID : CVE-2022-32929**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2448
Affected Version(s): * Up to (excluding) 15.7.1					
Buffer Copy	01-Nov-2022	9.8	The issue was addressed with	https://support.apple.com/	O-APP-IPAD-221122/2449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A buffer overflow may result in arbitrary code execution. **CVE ID : CVE-2022-32941**	en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32932**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2450
N/A	01-Nov-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and	https://support.apple.com/en-us/HT213490, https://support.apple.com/	O-APP-IPAD-221122/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32939**	en-us/HT213489	
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32944**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491	O-APP-IPAD-221122/2452
N/A	01-Nov-2022	7.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and	https://support.apple.com/en-us/HT213490, https://support.apple.com/	O-APP-IPAD-221122/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16. Joining a malicious Wi-Fi network may result in a denial-of-service of the Settings app. **CVE ID : CVE-2022-32927**	en-us/HT213489	
N/A	01-Nov-2022	6.7	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32926**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2454
N/A	01-Nov-2022	6.5	A correctness issue in the JIT was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://suppo	O-APP-IPAD-221122/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16. Processing maliciously crafted web content may disclose internal states of the app. **CVE ID : CVE-2022-32923**	rt.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	4.6	A lock screen issue was addressed with improved state management. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. A user may be able to view restricted content from the lock screen. **CVE ID : CVE-2022-32935**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2456
Affected Version(s): * Up to (excluding) 16.0					
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495	O-APP-IPAD-221122/2457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32922**	, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Big Sur 11.7, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32924**	https://support.apple.com/en-us/HT213443 , https://support.apple.com/en-us/HT213444 , https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2458
N/A	01-Nov-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS	https://support.apple.com/en-us/HT213488 , https://support.apple.com/	O-APP-IPAD-221122/2459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventura 13, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32940**	en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32947**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2460
Use After Free	01-Nov-2022	6.7	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42829**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Nov-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42830**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2462
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	6.4	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42831**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2463
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	6.4	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42832**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Nov-2022	5.5	This issue was addressed with improved entitlements. This issue is fixed in iOS 16.1 and iPadOS 16. An app may be able to record audio using a pair of connected AirPods. **CVE ID : CVE-2022-32946**	https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2465
N/A	01-Nov-2022	5.3	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. A shortcut may be able to check the existence of an arbitrary path on the file system. **CVE ID : CVE-2022-32938**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPAD-221122/2466
Affected Version(s): From (including) 15.0 Up to (excluding) 15.7					
N/A	01-Nov-2022	8.6	An access issue was addressed with improvements to the sandbox. This issue is fixed in Safari 16, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13. A sandboxed process may be able to circumvent	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213442, https://support.apple.com/en-	O-APP-IPAD-221122/2467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandbox restrictions. **CVE ID : CVE-2022-32892**	us/HT213445, https://support.apple.com/en-us/HT213446	
Product: iphone_os					
Affected Version(s): * Up to (excluding) 15.5					
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26709**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-IPHO-221122/2468
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, tvOS 15.5, watchOS 8.6. Processing	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://suppo	O-APP-IPHO-221122/2469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26710**	rt.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26716**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-IPHO-221122/2470
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5, iTunes	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://suppo	O-APP-IPHO-221122/2471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.12.4 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26717**	rt.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258, https://support.apple.com/en-us/HT213259	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26719**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-IPHO-221122/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2022-26762**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213258	O-APP-IPHO-221122/2473
N/A	01-Nov-2022	4.3	A logic issue in the handling of concurrent media was addressed with improved state handling. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. Video self-preview in a webRTC call may be interrupted if the user answers a phone call. **CVE ID : CVE-2022-22677**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213258	O-APP-IPHO-221122/2474
Affected Version(s): * Up to (excluding) 15.7					
Out-of-bounds Write	01-Nov-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487	O-APP-IPHO-221122/2475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.7, watchOS 9, macOS Monterey 12.6, tvOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32888**	, https://support.apple.com/en-us/HT213444 , https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213486 , https://support.apple.com/en-us/HT213445	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32898**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213486 , https://support.apple.com/en-us/HT213445 , https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2476
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue	https://support.apple.com/en-us/HT213488	O-APP-IPHO-221122/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32899**	, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	This issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.7 and iPadOS 15.7, macOS Ventura 13. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-42796**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213445	O-APP-IPHO-221122/2478
N/A	01-Nov-2022	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 15.7 and iPadOS 15.7, iOS 16.1 and iPadOS 16. An app may be able to access iOS backups. **CVE ID : CVE-2022-32929**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. A user may be able to view restricted content from the lock screen. **CVE ID : CVE-2022-42790**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2480
Improper Input Validation	01-Nov-2022	5.5	An issue in code signature validation was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. An app may be able to bypass code signing checks. **CVE ID : CVE-2022-42793**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213445,	O-APP-IPHO-221122/2481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	2.4	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, tvOS 16. A user with physical access to a device may be able to access contacts from the lock screen. **CVE ID : CVE-2022-32879**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2482
Affected Version(s): * Up to (excluding) 15.7.1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	9.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A buffer overflow may	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213493	O-APP-IPHO-221122/2483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in arbitrary code execution. **CVE ID : CVE-2022-32941**	, https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32932**	https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2484
N/A	01-Nov-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32939**	https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2485
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved state	https://support.apple.com/en-us/HT213488	O-APP-IPHO-221122/2486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32944**	, https://support.apple.com/en-us/HT213494 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213493 , https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491	
N/A	01-Nov-2022	7.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A user may be able to cause unexpected app termination or arbitrary code execution.	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213494 , https://support.apple.com/en-us/HT213493 , https://support.apple.com/en-us/HT213490	O-APP-IPHO-221122/2487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42800	, https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	
Out-of-bounds Write	01-Nov-2022	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-42827**	https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2488
N/A	01-Nov-2022	7.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. Joining a malicious Wi-Fi network may result in a denial-of-service of the Settings app.	https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32927		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	7	A race condition was addressed with improved locking. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42803**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2490
N/A	01-Nov-2022	6.7	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16. An app with root privileges may be	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/	O-APP-IPHO-221122/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32926**	en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	6.5	A correctness issue in the JIT was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose internal states of the app. **CVE ID : CVE-2022-32923**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2492
N/A	01-Nov-2022	6.5	A logic issue was addressed with	https://support.apple.com/	O-APP-IPHO-221122/2493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved state management. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS 9.1. Visiting a maliciously crafted website may leak sensitive data. **CVE ID : CVE-2022-42817**	en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. Parsing a maliciously crafted audio file may lead to disclosure of user information. **CVE ID : CVE-2022-42798**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491	O-APP-IPHO-221122/2494
N/A	01-Nov-2022	5.5	The issue was addressed with	https://support.apple.com/	O-APP-IPHO-221122/2495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing a maliciously crafted USD file may disclose memory contents. **CVE ID : CVE-2022-42810**	en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	4.6	A lock screen issue was addressed with improved state management. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. A user may be able to view restricted content from the lock screen. **CVE ID : CVE-2022-32935**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2496
Affected Version(s): * Up to (excluding) 16.0					
Out-of-bounds Write	01-Nov-2022	8.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 16, iOS 16, macOS Ventura 13, watchOS 9. Processing a	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213488,	O-APP-IPHO-221122/2497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2022-42795**	https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16, macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32865**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2498
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32887**	https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2499
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16, watchOS 9. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32889		
Use After Free	01-Nov-2022	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32903**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2501
N/A	01-Nov-2022	7.8	This issue was addressed with improved checks. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32907**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2502
Use After Free	01-Nov-2022	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-	O-APP-IPHO-221122/2503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with kernel privileges. **CVE ID : CVE-2022-32914**	us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
Out-of-bounds Write	01-Nov-2022	7.1	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2022-32925**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2504
N/A	01-Nov-2022	5.5	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 16, macOS Ventura 13. An app may be able to cause a denial-of-service.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32827		
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2022-32858**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2506
N/A	01-Nov-2022	5.5	The issue was addressed with improved handling of caches. This issue is fixed in iOS 16. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-32909**	https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2507
N/A	01-Nov-2022	5.5	This issue was addressed with improved data protection. This issue is fixed in iOS 16, macOS Ventura 13. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2022-32918**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2508
N/A	01-Nov-2022	5.3	A logic issue was addressed with improved state management. This	https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in iOS 16. Deleted contacts may still appear in spotlight search results. **CVE ID : CVE-2022-32859**		
N/A	01-Nov-2022	5.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. A user in a privileged network position may be able to intercept mail credentials. **CVE ID : CVE-2022-32928**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2510
N/A	01-Nov-2022	5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6. An app may be able to read sensitive location information. **CVE ID : CVE-2022-32875**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/	O-APP-IPHO-221122/2511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213446	
N/A	01-Nov-2022	3.3	This issue was addressed with improved entitlements. This issue is fixed in iOS 16, watchOS 9. An app may be able to read a persistent device identifier. **CVE ID : CVE-2022-32835**	https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2512
N/A	01-Nov-2022	3.3	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. A sandboxed app may be able to determine which app is currently using the camera. **CVE ID : CVE-2022-32913**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Nov-2022	2.4	This issue was addressed with improved data protection. This issue is fixed in iOS 16, macOS Ventura 13. A user with physical access to an iOS device may be able to read past diagnostic logs. **CVE ID : CVE-2022-32867**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2514
N/A	01-Nov-2022	2.4	A logic issue was addressed with improved state management. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. A user with physical access to a device may be able to use Siri to obtain some call history information. **CVE ID : CVE-2022-32870**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2515
Affected Version(s): * Up to (excluding) 5.7.1					
N/A	01-Nov-2022	7.8	A logic issue was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-	O-APP-IPHO-221122/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with kernel privileges. **CVE ID : CVE-2022-42801**	us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
Affected Version(s): From (including) 15.0 Up to (excluding) 15.7					
N/A	01-Nov-2022	8.6	An access issue was addressed with improvements to the sandbox. This issue is fixed in Safari 16, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2022-32892**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-221122/2517
Affected Version(s): * Up to (excluding) 16.0.3					
Improper Input Validation	01-Nov-2022	6.5	An input validation issue was addressed with improved input validation. This issue is fixed in iOS	https://support.apple.com/en-us/HT213480	O-APP-IPHO-221122/2518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.0.3. Processing a maliciously crafted email message may lead to a denial-of-service. **CVE ID : CVE-2022-22658**		
Affected Version(s): * Up to (excluding) 16.1					
Out-of-bounds Write	01-Nov-2022	9.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-42808**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2519
Improper Certificate Validation	01-Nov-2022	9.8	A certificate validation issue existed in the handling of WKWebView. This issue was addressed with improved validation. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. Processing a maliciously crafted	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://suppo	O-APP-IPHO-221122/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certificate may lead to arbitrary code execution. **CVE ID : CVE-2022-42813**	rt.apple.com/en-us/HT213489	
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32922**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2521
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-42823**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/	O-APP-IPHO-221122/2522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213489	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Big Sur 11.7, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32924**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2523
N/A	01-Nov-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to execute arbitrary	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/	O-APP-IPHO-221122/2524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with kernel privileges. **CVE ID : CVE-2022-32940**	en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32947**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2525
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app may cause unexpected app termination or arbitrary code execution. **CVE ID : CVE-2022-42820**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2526
Concurrent Execution using Shared Resource with	01-Nov-2022	7	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS	https://support.apple.com/en-us/HT213488, https://suppo	O-APP-IPHO-221122/2527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			Ventura 13. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42806**	rt.apple.com/en-us/HT213489	
Use After Free	01-Nov-2022	6.7	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42829**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2528
N/A	01-Nov-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42830**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2529
Concurrent Execution using Shared Resource with	01-Nov-2022	6.4	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS	https://support.apple.com/en-us/HT213488, https://suppo	O-APP-IPHO-221122/2530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42831**	rt.apple.com/en-us/HT213489	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	6.4	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42832**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2531
Improper Restriction of Rendered UI Layers or Frames	01-Nov-2022	6.1	The issue was addressed with improved UI handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Visiting a malicious website may lead to user interface spoofing. **CVE ID : CVE-2022-42799**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://suppo	O-APP-IPHO-221122/2532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rt.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	This issue was addressed with improved entitlements. This issue is fixed in iOS 16.1 and iPadOS 16. An app may be able to record audio using a pair of connected AirPods. **CVE ID : CVE-2022-32946**	https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2533
N/A	01-Nov-2022	5.5	An access issue was addressed with additional sandbox restrictions. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-42811**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2534
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state management. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495	O-APP-IPHO-221122/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16. Processing maliciously crafted web content may disclose sensitive user information. **CVE ID : CVE-2022-42824**	, https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	This issue was addressed by removing additional entitlements. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-42825**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213494 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213493 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/	O-APP-IPHO-221122/2536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213489	
N/A	01-Nov-2022	5.3	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. A shortcut may be able to check the existence of an arbitrary path on the file system. **CVE ID : CVE-2022-32938**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2537
Affected Version(s): 16.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	9.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A buffer overflow may result in arbitrary code execution. **CVE ID : CVE-2022-32941**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/	O-APP-IPHO-221122/2538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213489	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32932**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2539
N/A	01-Nov-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32939**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2540
Out-of-bounds Write	01-Nov-2022	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An application may be able to execute arbitrary code with	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-42827**		
N/A	01-Nov-2022	7.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. Joining a malicious Wi-Fi network may result in a denial-of-service of the Settings app. **CVE ID : CVE-2022-32927**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2542
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	7	A race condition was addressed with improved locking. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42803**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490,	O-APP-IPHO-221122/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	6.7	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32926**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2544
N/A	01-Nov-2022	6.5	A correctness issue in the JIT was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, Safari	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495,	O-APP-IPHO-221122/2545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose internal states of the app. **CVE ID : CVE-2022-32923**	https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS 9.1. Visiting a maliciously crafted website may leak sensitive data. **CVE ID : CVE-2022-42817**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2546
N/A	01-Nov-2022	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 15.7 and iPadOS 15.7, iOS 16.1 and iPadOS 16. An app may be able	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213445,	O-APP-IPHO-221122/2547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access iOS backups. **CVE ID : CVE-2022-32929**	https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing a maliciously crafted USD file may disclose memory contents. **CVE ID : CVE-2022-42810**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-IPHO-221122/2548
Product: macos					
Affected Version(s): * Up to (excluding) 12.6.1					
Out-of-bounds Write	01-Nov-2022	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been actively exploited.. **CVE ID : CVE-2022-42827**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	7	A race condition was addressed with improved locking. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42803**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2550
Affected Version(s): * Up to (excluding) 13.0					
Improper Certificate Validation	01-Nov-2022	9.8	A certificate validation issue existed in the handling of WKWebView. This issue was addressed with improved validation. This	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492	O-APP-MACO-221122/2551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. Processing a maliciously crafted certificate may lead to arbitrary code execution. **CVE ID : CVE-2022-42813**	, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
Out-of-bounds Write	01-Nov-2022	9.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-42808**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2552
N/A	01-Nov-2022	8.8	A memory corruption issue existed in the processing of ICC profiles. This issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13. Processing a maliciously crafted	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image may lead to arbitrary code execution. **CVE ID : CVE-2022-26730**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-42823**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2554
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32922		
Out-of-bounds Write	01-Nov-2022	8.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 16, iOS 16, macOS Ventura 13, watchOS 9. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2022-42795**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2556
N/A	01-Nov-2022	8.6	An access issue was addressed with improvements to the sandbox. This issue is fixed in Safari 16, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2022-32892**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2557
N/A	01-Nov-2022	8.6	A logic issue was addressed with improved checks.	https://support.apple.com/	O-APP-MACO-221122/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in macOS Ventura 13. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2022-32890**	en-us/HT213488	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. Processing a maliciously crafted gcx file may lead to unexpected app termination or arbitrary code execution. **CVE ID : CVE-2022-42809**	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2559
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app may cause unexpected app termination or arbitrary code execution. **CVE ID : CVE-2022-42820**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2560
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory	https://support.apple.com/en-	O-APP-MACO-221122/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling. This issue is fixed in iOS 16, macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32865**	us/HT213488, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Big Sur 11.7, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32924**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2562
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7	https://support.apple.com/en-us/HT213488,	O-APP-MACO-221122/2563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32898**	https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32940**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2564
N/A	01-Nov-2022	7.8	This issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.7 and iPadOS 15.7, macOS Ventura 13. An app may be able to gain elevated privileges.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213445	O-APP-MACO-221122/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42796		
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32947**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2566
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32899**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2567
Improper Link Resolution Before File Access ('Link Following')	01-Nov-2022	7.8	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13. Processing a	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted DMG file may lead to arbitrary code execution with system privileges. **CVE ID : CVE-2022-32905**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	7.8	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32915**	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2569
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	7	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42806**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2570
Concurrent Execution using Shared Resource with Improper Synchronization	01-Nov-2022	7	A race condition was addressed with improved state handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213488, https://support.apple.com/kb/HT213446	O-APP-MACO-221122/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			**CVE ID : CVE-2022-42791**		
N/A	01-Nov-2022	6.7	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32926**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2572
Use After Free	01-Nov-2022	6.7	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42829**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Nov-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42830**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2574
N/A	01-Nov-2022	6.5	A correctness issue in the JIT was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose internal states of the app. **CVE ID : CVE-2022-32923**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	6.4	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42832**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2576
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	6.4	A race condition was addressed with improved locking. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42831**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2577
Improper Restriction of Rendered UI Layers or Frames	01-Nov-2022	6.1	The issue was addressed with improved UI handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Visiting a malicious website may lead to user interface spoofing.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492,	O-APP-MACO-221122/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42799	https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.9	This issue was addressed with improved data protection. This issue is fixed in macOS Ventura 13. A user in a privileged network position may be able to track user activity. **CVE ID : CVE-2022-42818**	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2579
N/A	01-Nov-2022	5.5	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 16, macOS Ventura 13. An app may be able to cause a denial-of-service. **CVE ID : CVE-2022-32827**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2580
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. An app may be able to leak	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-	O-APP-MACO-221122/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive kernel state. **CVE ID : CVE-2022-32858**	us/HT213486, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	5.5	This issue was addressed with improved data protection. This issue is fixed in iOS 16, macOS Ventura 13. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2022-32918**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2582
Out-of-bounds Read	01-Nov-2022	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32936**	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2583
Incorrect Permission Assignment for Critical Resource	01-Nov-2022	5.5	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in macOS Ventura 13. A malicious application may be able to read sensitive location information.	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42788		
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing a maliciously crafted USD file may disclose memory contents. **CVE ID : CVE-2022-42810**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2585
N/A	01-Nov-2022	5.5	An access issue was addressed with additional sandbox restrictions. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-42811**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2586
N/A	01-Nov-2022	5.5	This issue was addressed with improved data	https://support.apple.com/	O-APP-MACO-221122/2587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection. This issue is fixed in macOS Ventura 13. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-42815**	en-us/HT213488	
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-42814**	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2588
N/A	01-Nov-2022	5.5	This issue was addressed by removing additional entitlements. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-42825**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213491,	O-APP-MACO-221122/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state management. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose sensitive user information. **CVE ID : CVE-2022-42824**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2590
N/A	01-Nov-2022	5.3	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13. A shortcut may be able to check the existence of an arbitrary path on the file system.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32938		
N/A	01-Nov-2022	5.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. A user in a privileged network position may be able to intercept mail credentials. **CVE ID : CVE-2022-32928**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2592
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Nov-2022	4.7	A race condition was addressed with improved state handling. This issue is fixed in macOS Ventura 13. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32895**	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2593
N/A	01-Nov-2022	4.6	A lock screen issue was addressed with improved state management. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. A user may be able to view restricted content from the lock screen.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32935		
N/A	01-Nov-2022	2.4	This issue was addressed with improved data protection. This issue is fixed in iOS 16, macOS Ventura 13. A user with physical access to an iOS device may be able to read past diagnostic logs. **CVE ID : CVE-2022-32867**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2595
N/A	01-Nov-2022	2.4	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, tvOS 16. A user with physical access to a device may be able to access contacts from the lock screen. **CVE ID : CVE-2022-32879**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2596
N/A	01-Nov-2022	2.4	A logic issue was addressed with improved state management. This	https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. A user with physical access to a device may be able to use Siri to obtain some call history information. **CVE ID : CVE-2022-32870**	, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
Affected Version(s): From (including) 11.0 Up to (excluding) 11.6.6					
N/A	01-Nov-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-32794**	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213255	O-APP-MACO-221122/2598
Affected Version(s): From (including) 11.0 Up to (excluding) 11.6.8					
N/A	01-Nov-2022	7.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.8, macOS Monterey 12.5, Security Update 2022-005 Catalina. An archive may be able to bypass Gatekeeper. **CVE ID : CVE-2022-32910**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-221122/2599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 11.0 Up to (excluding) 11.7					
Out-of-bounds Write	01-Nov-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, macOS Monterey 12.6, tvOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32888**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445	O-APP-MACO-221122/2600
N/A	01-Nov-2022	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-32934**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/	O-APP-MACO-221122/2601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213488	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32866**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486	O-APP-MACO-221122/2602
Use After Free	01-Nov-2022	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32914**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/	O-APP-MACO-221122/2603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Big Sur 11.7, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32924**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2604
N/A	01-Nov-2022	5.5	A configuration issue was	https://support.apple.com/	O-APP-MACO-221122/2605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addressed with additional restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Monterey 12.6. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-32877**	en-us/HT213443, https://support.apple.com/en-us/HT213444	
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32881**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2606
N/A	01-Nov-2022	5.5	An access issue was addressed with additional sandbox	https://support.apple.com/en-	O-APP-MACO-221122/2607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-32904**	us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488	
N/A	01-Nov-2022	5.5	An issue in code signature validation was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-42789**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2608
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. A user may be able to view restricted content from the lock screen. **CVE ID : CVE-2022-42790**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-	O-APP-MACO-221122/2609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213445 , https://support.apple.com/en-us/HT213446	
Improper Input Validation	01-Nov-2022	5.5	An issue in code signature validation was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. An app may be able to bypass code signing checks. **CVE ID : CVE-2022-42793**	https://support.apple.com/en-us/HT213443 , https://support.apple.com/en-us/HT213444 , https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213445 , https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2610
N/A	01-Nov-2022	5.5	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. An app may be able to read sensitive location information.	https://support.apple.com/en-us/HT213443 , https://support.apple.com/en-us/HT213444 , https://support.apple.com/	O-APP-MACO-221122/2611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42819	en-us/HT213488	
N/A	01-Nov-2022	5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6. An app may be able to read sensitive location information. **CVE ID : CVE-2022-32875**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2612
N/A	01-Nov-2022	3.3	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. A sandboxed app may be able to determine which app is currently using the camera.	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/	O-APP-MACO-221122/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32913	en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
Affected Version(s): From (including) 11.0 Up to (excluding) 11.7.1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	9.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A buffer overflow may result in arbitrary code execution. **CVE ID : CVE-2022-32941**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2614
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in	https://support.apple.com/en-us/HT213488, https://suppo	O-APP-MACO-221122/2615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32944**	rt.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491	
N/A	01-Nov-2022	7.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A user may be able to cause unexpected app termination or arbitrary code execution. **CVE ID : CVE-2022-42800**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://suppo	O-APP-MACO-221122/2616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rt.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	This issue was addressed with improved data protection. This issue is fixed in macOS Big Sur 11.7.1, macOS Ventura 13, macOS Monterey 12.6.1. An app with root privileges may be able to access private information. **CVE ID : CVE-2022-32862**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213493	O-APP-MACO-221122/2617
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. Parsing a maliciously crafted audio file may lead to disclosure of user information.	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493	O-APP-MACO-221122/2618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42798	, https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491	
N/A	01-Nov-2022	5.5	This issue was addressed by removing additional entitlements. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-42825**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213494 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213493 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2619
Affected Version(s): From (including) 12.0 Up to (excluding) 12.5					
N/A	01-Nov-2022	7.5	A logic issue was addressed with improved checks.	https://support.apple.com/en-	O-APP-MACO-221122/2620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in macOS Big Sur 11.6.8, macOS Monterey 12.5, Security Update 2022-005 Catalina. An archive may be able to bypass Gatekeeper. **CVE ID : CVE-2022-32910**	us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	
Affected Version(s): From (including) 12.0 Up to (excluding) 12.6					
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32866**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486	O-APP-MACO-221122/2621
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Big Sur 11.7, macOS	https://support.apple.com/en-us/HT213443, https://support.apple.com/	O-APP-MACO-221122/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32924**	en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	A configuration issue was addressed with additional restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Monterey 12.6. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-32877**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444	O-APP-MACO-221122/2623
N/A	01-Nov-2022	5.5	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-	O-APP-MACO-221122/2624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-32904**	us/HT213444, https://support.apple.com/en-us/HT213488	
N/A	01-Nov-2022	5.5	An issue in code signature validation was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-42789**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2625
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. A user may be able to view restricted content from the lock screen. **CVE ID : CVE-2022-42790**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213445, https://support.apple.com/	O-APP-MACO-221122/2626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213446	
Improper Input Validation	01-Nov-2022	5.5	An issue in code signature validation was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, macOS Monterey 12.6. An app may be able to bypass code signing checks. **CVE ID : CVE-2022-42793**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2627
N/A	01-Nov-2022	5.5	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. An app may be able to read sensitive location information. **CVE ID : CVE-2022-42819**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488	O-APP-MACO-221122/2628
N/A	01-Nov-2022	5	A logic issue was addressed with improved state	https://support.apple.com/en-	O-APP-MACO-221122/2629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6. An app may be able to read sensitive location information. **CVE ID : CVE-2022-32875**	us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
Affected Version(s): From (including) 12.0 Up to (excluding) 12.6.1					
N/A	01-Nov-2022	7.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A user may be able to cause unexpected app termination or arbitrary code execution. **CVE ID : CVE-2022-42800**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://suppo	O-APP-MACO-221122/2630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rt.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	A logic issue was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42801**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2631
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, iOS 15.7.1 and	https://support.apple.com/en-us/HT213488, https://suppo	O-APP-MACO-221122/2632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. Parsing a maliciously crafted audio file may lead to disclosure of user information. **CVE ID : CVE-2022-42798**	rt.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491	
N/A	01-Nov-2022	5.5	This issue was addressed by removing additional entitlements. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-42825**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://suppo	O-APP-MACO-221122/2633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rt.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.4					
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26709**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-MACO-221122/2634
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, tvOS 15.5, watchOS	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254,	O-APP-MACO-221122/2635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26710**	https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26716**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-MACO-221122/2636
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4,	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254,	O-APP-MACO-221122/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Safari 15.5, iTunes 12.12.4 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26717**	https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258, https://support.apple.com/en-us/HT213259	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26719**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-MACO-221122/2638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2022-26762**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213258	O-APP-MACO-221122/2639
N/A	01-Nov-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-32794**	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213255	O-APP-MACO-221122/2640
N/A	01-Nov-2022	4.3	A logic issue in the handling of concurrent media was addressed with improved state handling. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5. Video self-preview in a webRTC call may be interrupted if	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213258	O-APP-MACO-221122/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the user answers a phone call. **CVE ID : CVE-2022-22677**		
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.6					
Out-of-bounds Write	01-Nov-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, macOS Monterey 12.6, tvOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32888**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445	O-APP-MACO-221122/2642
N/A	01-Nov-2022	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, macOS Monterey 12.6. A remote user may be	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444	O-APP-MACO-221122/2643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to cause kernel code execution. **CVE ID : CVE-2022-32934**	, https://support.apple.com/en-us/HT213488	
Use After Free	01-Nov-2022	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32914**	https://support.apple.com/en-us/HT213443 , https://support.apple.com/en-us/HT213487 , https://support.apple.com/en-us/HT213444 , https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213486 , https://support.apple.com/en-us/HT213446	O-APP-MACO-221122/2644
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey	https://support.apple.com/en-us/HT213443 , https://support.apple.com/en-us/HT213487	O-APP-MACO-221122/2645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6, tvOS 16. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32881**	, https://support.apple.com/en-us/HT213444 , https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213486 , https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	3.3	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. A sandboxed app may be able to determine which app is currently using the camera. **CVE ID : CVE-2022-32913**	https://support.apple.com/en-us/HT213443 , https://support.apple.com/en-us/HT213487 , https://support.apple.com/en-us/HT213444 , https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213486	O-APP-MACO-221122/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				, https://support.apple.com/en-us/HT213446	
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.6.1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	9.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A buffer overflow may result in arbitrary code execution. **CVE ID : CVE-2022-32941**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213494 , https://support.apple.com/en-us/HT213493 , https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213489	O-APP-MACO-221122/2647
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213494 , https://support.apple.com/en-	O-APP-MACO-221122/2648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6.1, macOS Big Sur 11.7.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32944**	us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491	
N/A	01-Nov-2022	5.5	This issue was addressed with improved data protection. This issue is fixed in macOS Big Sur 11.7.1, macOS Ventura 13, macOS Monterey 12.6.1. An app with root privileges may be able to access private information. **CVE ID : CVE-2022-32862**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213493	O-APP-MACO-221122/2649
Product: mac_os_x					
Affected Version(s): 10.15.7					
N/A	01-Nov-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-	O-APP-MAC_-221122/2650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.4, macOS Big Sur 11.6.6. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-32794**	us/HT213257, https://support.apple.com/en-us/HT213255	
N/A	01-Nov-2022	7.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.8, macOS Monterey 12.5, Security Update 2022-005 Catalina. An archive may be able to bypass Gatekeeper. **CVE ID : CVE-2022-32910**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MAC_-221122/2651
Affected Version(s): From (including) 10.15 Up to (excluding) 10.15.7					
N/A	01-Nov-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2022-004 Catalina, macOS Monterey 12.4, macOS Big Sur 11.6.6. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-32794**	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213255	O-APP-MAC_-221122/2652
N/A	01-Nov-2022	7.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.8, macOS Monterey 12.5,	https://support.apple.com/en-us/HT213344, https://support.apple.com/	O-APP-MAC_-221122/2653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Update 2022-005 Catalina. An archive may be able to bypass Gatekeeper. **CVE ID : CVE-2022-32910**	en-us/HT213345, https://support.apple.com/en-us/HT213343	
Product: tvos					
Affected Version(s): * Up to (excluding) 15.5					
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26709**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-TVOS-221122/2654
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4,	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254	O-APP-TVOS-221122/2655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tvOS 15.5, watchOS 8.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26710**	, https://support.apple.com/en-us/HT213253 , https://support.apple.com/en-us/HT213258	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26716**	https://support.apple.com/en-us/HT213257 , https://support.apple.com/en-us/HT213254 , https://support.apple.com/en-us/HT213253 , https://support.apple.com/en-us/HT213260 , https://support.apple.com/en-us/HT213258	O-APP-TVOS-221122/2656
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS	https://support.apple.com/en-us/HT213257 , https://support.apple.com/en-us/HT213254	O-APP-TVOS-221122/2657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Monterey 12.4, Safari 15.5, iTunes 12.12.4 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26717**	, https://support.apple.com/en-us/HT213253 , https://support.apple.com/en-us/HT213260 , https://support.apple.com/en-us/HT213258 , https://support.apple.com/en-us/HT213259	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26719**	https://support.apple.com/en-us/HT213257 , https://support.apple.com/en-us/HT213254 , https://support.apple.com/en-us/HT213253 , https://support.apple.com/en-us/HT213260 , https://support.apple.com/	O-APP-TVOS-221122/2658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213258	
Affected Version(s): * Up to (excluding) 16.0					
Out-of-bounds Write	01-Nov-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, macOS Monterey 12.6, tvOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32888**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445	O-APP-TVOS-221122/2659
Out-of-bounds Write	01-Nov-2022	8.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 16, iOS 16, macOS Ventura 13, watchOS 9. Processing a maliciously crafted	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213488, https://suppo	O-APP-TVOS-221122/2660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image may lead to arbitrary code execution. **CVE ID : CVE-2022-42795**	rt.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32866**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486	O-APP-TVOS-221122/2661
Use After Free	01-Nov-2022	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to execute arbitrary	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213486, https://suppo	O-APP-TVOS-221122/2662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with kernel privileges. **CVE ID : CVE-2022-32903**	rt.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	This issue was addressed with improved checks. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32907**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-TVOS-221122/2663
Use After Free	01-Nov-2022	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32914**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486,	O-APP-TVOS-221122/2664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213446	
Out-of-bounds Write	01-Nov-2022	7.1	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2022-32925**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-TVOS-221122/2665
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32881**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486	O-APP-TVOS-221122/2666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	3.3	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. A sandboxed app may be able to determine which app is currently using the camera. **CVE ID : CVE-2022-32913**	https://support.apple.com/en-us/HT213443 , https://support.apple.com/en-us/HT213487 , https://support.apple.com/en-us/HT213444 , https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213486 , https://support.apple.com/en-us/HT213446	O-APP-TVOS-221122/2667
N/A	01-Nov-2022	2.4	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, tvOS 16.	https://support.apple.com/en-us/HT213487 , https://support.apple.com/en-us/HT213488	O-APP-TVOS-221122/2668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A user with physical access to a device may be able to access contacts from the lock screen. **CVE ID : CVE-2022-32879**	, https://support.apple.com/en-us/HT213486 , https://support.apple.com/en-us/HT213445 , https://support.apple.com/en-us/HT213446	
Affected Version(s): * Up to (excluding) 16.1					
Out-of-bounds Write	01-Nov-2022	9.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-42808**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	O-APP-TVOS-221122/2669
Improper Certificate Validation	01-Nov-2022	9.8	A certificate validation issue existed in the handling of WKWebView. This issue was addressed with improved	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-	O-APP-TVOS-221122/2670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. Processing a maliciously crafted certificate may lead to arbitrary code execution. **CVE ID : CVE-2022-42813**	us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-42823**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-TVOS-221122/2671
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Big Sur	https://support.apple.com/en-us/HT213443, https://suppo	O-APP-TVOS-221122/2672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.7, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32924**	rt.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32940**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-TVOS-221122/2673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32944**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491	O-APP-TVOS-221122/2674
N/A	01-Nov-2022	7.8	A logic issue was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492,	O-APP-TVOS-221122/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with kernel privileges. **CVE ID : CVE-2022-42801**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
Out-of-bounds Write	01-Nov-2022	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-42827**	https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	O-APP-TVOS-221122/2676
Concurrent Execution using Shared Resource with Improper Synchronization	01-Nov-2022	7	A race condition was addressed with improved locking. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494	O-APP-TVOS-221122/2677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42803**	, https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	6.7	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32926**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/	O-APP-TVOS-221122/2678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213489	
N/A	01-Nov-2022	6.5	A correctness issue in the JIT was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose internal states of the app. **CVE ID : CVE-2022-32923**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-TVOS-221122/2679
Improper Restriction of Rendered UI Layers or Frames	01-Nov-2022	6.1	The issue was addressed with improved UI handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Visiting a malicious website	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/	O-APP-TVOS-221122/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to user interface spoofing. **CVE ID : CVE-2022-42799**	en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. Parsing a maliciously crafted audio file may lead to disclosure of user information. **CVE ID : CVE-2022-42798**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491	O-APP-TVOS-221122/2681
N/A	01-Nov-2022	5.5	The issue was addressed with	https://support.apple.com/	O-APP-TVOS-221122/2682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13. Processing a maliciously crafted USD file may disclose memory contents. **CVE ID : CVE-2022-42810**	en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	An access issue was addressed with additional sandbox restrictions. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-42811**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-TVOS-221122/2683
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state management. This issue is fixed in tvOS 16.1, macOS Ventura 13,	https://support.apple.com/en-us/HT213488, https://support.apple.com/	O-APP-TVOS-221122/2684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose sensitive user information. **CVE ID : CVE-2022-42824**	en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	This issue was addressed by removing additional entitlements. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-42825**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213491, https://support.apple.com/	O-APP-TVOS-221122/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213489	
Product: watchos					
Affected Version(s): * Up to (excluding) 8.6					
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26709**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-WATC-221122/2686
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, tvOS 15.5, watchOS 8.6. Processing maliciously crafted web content may	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253,	O-APP-WATC-221122/2687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2022-26710**	https://support.apple.com/en-us/HT213258	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26716**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-WATC-221122/2688
Use After Free	01-Nov-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5, iTunes 12.12.4 for Windows. Processing maliciously crafted	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253,	O-APP-WATC-221122/2689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26717**	https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258, https://support.apple.com/en-us/HT213259	
N/A	01-Nov-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, iOS 15.5 and iPadOS 15.5, watchOS 8.6, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-26719**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-WATC-221122/2690
Affected Version(s): * Up to (excluding) 9.0					
Out-of-bounds Write	01-Nov-2022	8.8	An out-of-bounds write issue was addressed with improved bounds	https://support.apple.com/en-us/HT213443	O-APP-WATC-221122/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, macOS Monterey 12.6, tvOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32888**	, https://support.apple.com/en-us/HT213487 , https://support.apple.com/en-us/HT213444 , https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213486 , https://support.apple.com/en-us/HT213445	
Out-of-bounds Write	01-Nov-2022	8.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 16, iOS 16, macOS Ventura 13, watchOS 9. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2022-42795**	https://support.apple.com/en-us/HT213487 , https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213486 , https://support.apple.com/	O-APP-WATC-221122/2692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213446	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32866**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486	O-APP-WATC-221122/2693
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32889**	https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-WATC-221122/2694
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7	https://support.apple.com/en-us/HT213488,	O-APP-WATC-221122/2695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32898**	https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Ventura 13, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32899**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-WATC-221122/2696
Use After Free	01-Nov-2022	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to execute arbitrary	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213486,	O-APP-WATC-221122/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with kernel privileges. **CVE ID : CVE-2022-32903**	https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	7.8	This issue was addressed with improved checks. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32907**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-WATC-221122/2698
Use After Free	01-Nov-2022	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32914**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486,	O-APP-WATC-221122/2699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213446	
Out-of-bounds Write	01-Nov-2022	7.1	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 16, iOS 16, watchOS 9. An app may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2022-32925**	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-WATC-221122/2700
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2022-32858**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-WATC-221122/2701
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. An	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487,	O-APP-WATC-221122/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32881**	https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	5.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. A user in a privileged network position may be able to intercept mail credentials. **CVE ID : CVE-2022-32928**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-WATC-221122/2703
N/A	01-Nov-2022	5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6. An app may	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444,	O-APP-WATC-221122/2704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be able to read sensitive location information. **CVE ID : CVE-2022-32875**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	3.3	This issue was addressed with improved entitlements. This issue is fixed in iOS 16, watchOS 9. An app may be able to read a persistent device identifier. **CVE ID : CVE-2022-32835**	https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-WATC-221122/2705
N/A	01-Nov-2022	3.3	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Big Sur 11.7, macOS Ventura 13, iOS 16, watchOS 9, macOS Monterey 12.6, tvOS 16. A sandboxed app may be able to determine which app is currently using the camera.	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-	O-APP-WATC-221122/2706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32913	us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	
N/A	01-Nov-2022	2.4	A logic issue was addressed with improved state management. This issue is fixed in iOS 16, macOS Ventura 13, watchOS 9. A user with physical access to a device may be able to use Siri to obtain some call history information. **CVE ID : CVE-2022-32870**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/en-us/HT213446	O-APP-WATC-221122/2707
N/A	01-Nov-2022	2.4	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13, iOS 16, iOS 15.7 and iPadOS 15.7, watchOS 9, tvOS 16. A user with physical access to a device may be able to access contacts from the lock screen.	https://support.apple.com/en-us/HT213487, https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213486, https://support.apple.com/	O-APP-WATC-221122/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32879	en-us/HT213445, https://support.apple.com/en-us/HT213446	
Affected Version(s): * Up to (excluding) 9.1					
Out-of-bounds Write	01-Nov-2022	9.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-42808**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-WATC-221122/2709
Improper Certificate Validation	01-Nov-2022	9.8	A certificate validation issue existed in the handling of WKWebView. This issue was addressed with improved validation. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. Processing a maliciously crafted	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://suppo	O-APP-WATC-221122/2710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certificate may lead to arbitrary code execution. **CVE ID : CVE-2022-42813**	rt.apple.com/en-us/HT213489	
Access of Resource Using Incompatible Type ('Type Confusion')	01-Nov-2022	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-42823**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-WATC-221122/2711
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, macOS Big Sur 11.7, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6. An app may be able to execute	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213488	O-APP-WATC-221122/2712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with kernel privileges. **CVE ID : CVE-2022-32924**	, https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32932**	https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	O-APP-WATC-221122/2713
N/A	01-Nov-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213491	O-APP-WATC-221122/2714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32940	, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32944**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213494 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213493 , https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491	O-APP-WATC-221122/2715
N/A	01-Nov-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213491	O-APP-WATC-221122/2716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32947**	, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	7.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. A user may be able to cause unexpected app termination or arbitrary code execution. **CVE ID : CVE-2022-42800**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213494 , https://support.apple.com/en-us/HT213493 , https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	O-APP-WATC-221122/2717
N/A	01-Nov-2022	7.8	A logic issue was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213494	O-APP-WATC-221122/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42801**	, https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	
Out-of-bounds Write	01-Nov-2022	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-42827**	https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213489	O-APP-WATC-221122/2719
Concurrent Execution using	01-Nov-2022	7	A race condition was addressed with improved locking.	https://support.apple.com/en-	O-APP-WATC-221122/2720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-42803**	us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	6.7	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32926**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-	O-APP-WATC-221122/2721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213491 , https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	6.5	A correctness issue in the JIT was addressed with improved checks. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose internal states of the app. **CVE ID : CVE-2022-32923**	https://support.apple.com/en-us/HT213488 , https://support.apple.com/en-us/HT213495 , https://support.apple.com/en-us/HT213492 , https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-us/HT213491 , https://support.apple.com/en-us/HT213489	O-APP-WATC-221122/2722
N/A	01-Nov-2022	6.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.7.1 and iPadOS 15.7.1, iOS 16.1 and iPadOS 16, watchOS	https://support.apple.com/en-us/HT213490 , https://support.apple.com/en-	O-APP-WATC-221122/2723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.1. Visiting a maliciously crafted website may leak sensitive data. **CVE ID : CVE-2022-42817**	us/HT213491, https://support.apple.com/en-us/HT213489	
Improper Restriction of Rendered UI Layers or Frames	01-Nov-2022	6.1	The issue was addressed with improved UI handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Visiting a malicious website may lead to user interface spoofing. **CVE ID : CVE-2022-42799**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-WATC-221122/2724
N/A	01-Nov-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.1, iOS 15.7.1 and iPadOS 15.7.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. Parsing	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-	O-APP-WATC-221122/2725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a maliciously crafted audio file may lead to disclosure of user information. **CVE ID : CVE-2022-42798**	us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213490, https://support.apple.com/en-us/HT213491	
N/A	01-Nov-2022	5.5	An access issue was addressed with additional sandbox restrictions. This issue is fixed in tvOS 16.1, iOS 16.1 and iPadOS 16, macOS Ventura 13, watchOS 9.1. An app may be able to access user-sensitive data. **CVE ID : CVE-2022-42811**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	O-APP-WATC-221122/2726
N/A	01-Nov-2022	5.5	A logic issue was addressed with improved state management. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-	O-APP-WATC-221122/2727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.1, iOS 16.1 and iPadOS 16. Processing maliciously crafted web content may disclose sensitive user information. **CVE ID : CVE-2022-42824**	us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213491, https://support.apple.com/en-us/HT213489	
N/A	01-Nov-2022	5.5	This issue was addressed by removing additional entitlements. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, iOS 16.1 and iPadOS 16, macOS Monterey 12.6.1, macOS Big Sur 11.7.1. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-42825**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213494, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-us/HT213493, https://support.apple.com/en-us/HT213491, https://support.apple.com/	O-APP-WATC-221122/2728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213489	
Vendor: Avaya					
Product: scopia_pathfinder_10_pts_firmware					
Affected Version(s): 8.3.7.0.4					
Missing Authentication for Critical Function	03-Nov-2022	9.1	** UNSUPPPORTED WHEN ASSIGNED **Broken Access Control in User Authentication in Avaya Scopia Pathfinder 10 and 20 PTS version 8.3.7.0.4 allows remote unauthenticated attackers to bypass the login page, access sensitive information, and reset user passwords via URL modification. **CVE ID : CVE-2022-38168**	N/A	O-AVA-SCOP-221122/2729
Product: scopia_pathfinder_20_pts_firmware					
Affected Version(s): 8.3.7.0.4					
Missing Authentication for Critical Function	03-Nov-2022	9.1	** UNSUPPPORTED WHEN ASSIGNED **Broken Access Control in User Authentication in Avaya Scopia Pathfinder 10 and 20 PTS version 8.3.7.0.4 allows remote unauthenticated attackers to bypass the login page, access sensitive	N/A	O-AVA-SCOP-221122/2730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information, and reset user passwords via URL modification. **CVE ID : CVE-2022-38168**		
Vendor: BD					
Product: totalys_multiprocessor_firmware					
Affected Version(s): * Up to (excluding) 1.71					
Use of Hard-coded Credentials	04-Nov-2022	7.8	BD Totalys MultiProcessor, versions 1.70 and earlier, contain hardcoded credentials. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII). Customers using BD Totalys MultiProcessor version 1.70 with Microsoft Windows 10 have additional operating system hardening configurations which increase the attack complexity required to exploit this vulnerability.	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-totalys-multiprocessor-hardcoded-credentials	O-BD-TOTA-221122/2731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40263		
Vendor: Canonical					
Product: ubuntu_linux					
Affected Version(s): 18.04					
N/A	06-Nov-2022	9.8	Mahara 21.04 before 21.04.7, 21.10 before 21.10.5, 22.04 before 22.04.3, and 22.10 before 22.10.0 potentially allow a PDF export to trigger a remote shell if the site is running on Ubuntu and the flag -dSAFER is not set with Ghostscript. **CVE ID : CVE-2022-44544**	https://bugs.launchpad.net/mahara/+bug/1979575, https://mahara.org/interaction/forum/topic.php?id=9198	O-CAN-UBUN-221122/2732
Vendor: Cisco					
Product: asyncos					
Affected Version(s): * Up to (excluding) 12.0.5-011					
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	O-CIS-ASYN-221122/2733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information from an affected device, including user credentials. This vulnerability is due to weak enforcement of back-end authorization checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Affected Version(s): * Up to (excluding) 14.2.0-217					
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive information from an affected device,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	O-CIS-ASYN-221122/2734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including user credentials. This vulnerability is due to weak enforcement of back-end authorization checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Affected Version(s): * Up to (excluding) 14.2.1-015					
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive information from an affected device, including user credentials. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	O-CIS-ASYN-221122/2735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to weak enforcement of back-end authorization checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Affected Version(s): 14.5					
Use of Hard-coded Credentials	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Email Security Appliance, Cisco Secure Email and Web Manager and Cisco Secure Web Appliance could allow an authenticated, remote attacker to elevate privileges on an affected system. The attacker needs valid credentials to exploit this vulnerability. This vulnerability is due to the use of a hardcoded value to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	O-CIS-ASYN-221122/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encrypt a token used for certain APIs calls . An attacker could exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to impersonate another valid user and execute commands with the privileges of that user account. **CVE ID : CVE-2022-20868**		
Affected Version(s): From (including) 11.8 Up to (excluding) 12.5.5					
Use of Hard-coded Credentials	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Email Security Appliance, Cisco Secure Email and Web Manager and Cisco Secure Web Appliance could allow an authenticated, remote attacker to elevate privileges on an affected system. The attacker needs valid credentials to exploit this vulnerability. This vulnerability is due	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	O-CIS-ASYN-221122/2737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the use of a hardcoded value to encrypt a token used for certain APIs calls . An attacker could exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to impersonate another valid user and execute commands with the privileges of that user account. **CVE ID : CVE-2022-20868**		
Affected Version(s): From (including) 12.0 Up to (excluding) 14.2.0					
Use of Hard-coded Credentials	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Email Security Appliance, Cisco Secure Email and Web Manager and Cisco Secure Web Appliance could allow an authenticated, remote attacker to elevate privileges on an affected system. The attacker needs valid credentials to exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	O-CIS-ASYN-221122/2738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability is due to the use of a hardcoded value to encrypt a token used for certain APIs calls . An attacker could exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to impersonate another valid user and execute commands with the privileges of that user account. **CVE ID : CVE-2022-20868**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Nov-2022	6.5	A vulnerability in web-based management interface of the of Cisco Email Security Appliance and Cisco Secure Email and Web Manager could allow an authenticated, remote attacker to conduct SQL injection attacks as root on an affected system. The attacker must have the credentials of a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	O-CIS-ASYN-221122/2739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high-privileged user account. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database of the affected system. **CVE ID : CVE-2022-20867**		
Affected Version(s): From (including) 12.5 Up to (excluding) 12.5.4-005					
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	O-CIS-ASYN-221122/2740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information from an affected device, including user credentials. This vulnerability is due to weak enforcement of back-end authorization checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Affected Version(s): From (including) 13.0 Up to (excluding) 14.2.1					
Use of Hard-coded Credentials	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Email Security Appliance, Cisco Secure Email and Web Manager and Cisco Secure Web Appliance could allow an authenticated, remote attacker to elevate privileges on an affected system. The attacker needs valid credentials to exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	O-CIS-ASYN-221122/2741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability is due to the use of a hardcoded value to encrypt a token used for certain APIs calls . An attacker could exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to impersonate another valid user and execute commands with the privileges of that user account. **CVE ID : CVE-2022-20868**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Nov-2022	6.5	A vulnerability in web-based management interface of the of Cisco Email Security Appliance and Cisco Secure Email and Web Manager could allow an authenticated, remote attacker to conduct SQL injection attacks as root on an affected system. The attacker must have the credentials of a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	O-CIS-ASYN-221122/2742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high-privileged user account. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database of the affected system. **CVE ID : CVE-2022-20867**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0.2-012					
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	O-CIS-ASYN-221122/2743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information from an affected device, including user credentials. This vulnerability is due to weak enforcement of back-end authorization checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0.4					
Use of Hard-coded Credentials	04-Nov-2022	8.8	A vulnerability in the web-based management interface of Cisco Email Security Appliance, Cisco Secure Email and Web Manager and Cisco Secure Web Appliance could allow an authenticated, remote attacker to elevate privileges on an affected system. The attacker needs valid credentials to exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD	O-CIS-ASYN-221122/2744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability is due to the use of a hardcoded value to encrypt a token used for certain APIs calls . An attacker could exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to impersonate another valid user and execute commands with the privileges of that user account. **CVE ID : CVE-2022-20868**		
Affected Version(s): From (including) 14.3.0 Up to (excluding) 14.3.0-023					
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	O-CIS-ASYN-221122/2745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information from an affected device, including user credentials. This vulnerability is due to weak enforcement of back-end authorization checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Affected Version(s): From (including) 14.3.0 Up to (excluding) 14.3.0-115					
Incorrect Authorization	04-Nov-2022	6.5	A vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance, formerly known as Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to retrieve sensitive information from an affected device,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG	O-CIS-ASYN-221122/2746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including user credentials. This vulnerability is due to weak enforcement of back-end authorization checks. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain confidential data that is stored on the affected device. **CVE ID : CVE-2022-20942**		
Product: email_security_appliance_firmware					
Affected Version(s): From (including) 13.5.1 Up to (excluding) 14.0.3-015					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Nov-2022	5.3	A vulnerability in Cisco Email Security Appliance (ESA) and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. This vulnerability is due to the failure of the application or its environment to properly sanitize input values. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-HTTP-Inject-nvsycUmR	O-CIS-EMAI-221122/2747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by injecting malicious HTTP headers, controlling the response body, or splitting the response into multiple responses. **CVE ID : CVE-2022-20772**		
Affected Version(s): From (including) 14.1 Up to (excluding) 14.2.1-015					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Nov-2022	5.3	A vulnerability in Cisco Email Security Appliance (ESA) and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. This vulnerability is due to the failure of the application or its environment to properly sanitize input values. An attacker could exploit this vulnerability by injecting malicious HTTP headers, controlling the response body, or splitting the response into multiple responses. **CVE ID : CVE-2022-20772**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-HTTP-Inject-nvsycUmR	O-CIS-EMAI-221122/2748
Affected Version(s): From (including) 14.3 Up to (excluding) 14.3.0-023					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Nov-2022	5.3	A vulnerability in Cisco Email Security Appliance (ESA) and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. This vulnerability is due to the failure of the application or its environment to properly sanitize input values. An attacker could exploit this vulnerability by injecting malicious HTTP headers, controlling the response body, or splitting the response into multiple responses. **CVE ID : CVE-2022-20772**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-HTTP-Inject-nvsycUmR	O-CIS-EMAI-221122/2749
Product: secure_email_and_web_manager_firmware					
Affected Version(s): From (including) 14.2 Up to (excluding) 14.2.0-217					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	04-Nov-2022	5.3	A vulnerability in Cisco Email Security Appliance (ESA) and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to conduct an HTTP response splitting	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-HTTP-Inject-nvsycUmR	O-CIS-SECU-221122/2750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			attack. This vulnerability is due to the failure of the application or its environment to properly sanitize input values. An attacker could exploit this vulnerability by injecting malicious HTTP headers, controlling the response body, or splitting the response into multiple responses. **CVE ID : CVE-2022-20772**		
Affected Version(s): From (including) 14.3 Up to (excluding) 14.3.0-115					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Nov-2022	5.3	A vulnerability in Cisco Email Security Appliance (ESA) and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. This vulnerability is due to the failure of the application or its environment to properly sanitize input values. An attacker could exploit this vulnerability by injecting malicious HTTP headers,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-HTTP-Inject-nvsycUmR	O-CIS-SECU-221122/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlling the response body, or splitting the response into multiple responses. **CVE ID : CVE-2022-20772**		
Vendor: Citrix					
Product: application_delivery_controller_firmware					
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-55.289					
Improper Authentication	08-Nov-2022	9.8	Unauthorized access to Gateway user capabilities **CVE ID : CVE-2022-27510**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	O-CIT-APPL-221122/2752
Improper Restriction of Excessive Authentication Attempts	08-Nov-2022	9.8	User login brute force protection functionality bypass **CVE ID : CVE-2022-27516**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	O-CIT-APPL-221122/2753
Insufficient Verification of Data	08-Nov-2022	9.6	Remote desktop takeover via phishing	https://support.citrix.com/article/CTX463706/citrix-	O-CIT-APPL-221122/2754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			**CVE ID : CVE-2022-27513**	gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-65.21					
Improper Authentication	08-Nov-2022	9.8	Unauthorized access to Gateway user capabilities **CVE ID : CVE-2022-27510**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	O-CIT-APPL-221122/2755
Improper Restriction of Excessive Authentication Attempts	08-Nov-2022	9.8	User login brute force protection functionality bypass **CVE ID : CVE-2022-27516**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	O-CIT-APPL-221122/2756
Insufficient Verification of Data	08-Nov-2022	9.6	Remote desktop takeover via phishing	https://support.citrix.com/article/CTX463706/citrix-	O-CIT-APPL-221122/2757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			**CVE ID : CVE-2022-27513**	gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-88.12					
Improper Authentication	08-Nov-2022	9.8	Unauthorized access to Gateway user capabilities **CVE ID : CVE-2022-27510**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	O-CIT-APPL-221122/2758
Improper Restriction of Excessive Authentication Attempts	08-Nov-2022	9.8	User login brute force protection functionality bypass **CVE ID : CVE-2022-27516**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	O-CIT-APPL-221122/2759
Insufficient Verification of Data	08-Nov-2022	9.6	Remote desktop takeover via phishing	https://support.citrix.com/article/CTX463706/citrix-	O-CIT-APPL-221122/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			**CVE ID : CVE-2022-27513**	gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-33.47					
Improper Authentication	08-Nov-2022	9.8	Unauthorized access to Gateway user capabilities **CVE ID : CVE-2022-27510**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	O-CIT-APPL-221122/2761
Improper Restriction of Excessive Authentication Attempts	08-Nov-2022	9.8	User login brute force protection functionality bypass **CVE ID : CVE-2022-27516**	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve20222751 0-cve20222751 3-and-cve20222751 6	O-CIT-APPL-221122/2762
Insufficient Verification of Data	08-Nov-2022	9.6	Remote desktop takeover via phishing	https://support.citrix.com/article/CTX463706/citrix-	O-CIT-APPL-221122/2763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			**CVE ID : CVE-2022-27513**	gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516	
Product: hypervisor					
Affected Version(s): -					
NULL Pointer Dereference	10-Nov-2022	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2022-34666**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	O-CIT-HYPE-221122/2764
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Incorrect Calculation of Buffer Size	08-Nov-2022	9.8	sysstat is a set of system performance tools for the Linux operating system. On 32 bit systems, in versions 9.1.16 and newer but prior to 12.7.1, allocate_structures contains a size_t	https://github.com/sysstat/sysstat/security/advisories/GHSA-q8r6-g56f-9w7x	O-DEB-DEBI-221122/2765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow in sa_common.c. The allocate_structures function insufficiently checks bounds before arithmetic multiplication, allowing for an overflow in the size allocated for the buffer representing system activities. This issue may lead to Remote Code Execution (RCE). This issue has been patched in version 12.7.1. **CVE ID : CVE-2022-39377**		
Vendor: Dlink					
Product: dir-823g_firmware					
Affected Version(s): 1.0.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Nov-2022	9.8	D-Link DIR-823G v1.0.2 was found to contain a command injection vulnerability in the function SetNetworkTomographySettings. This vulnerability allows attackers to execute arbitrary commands via a crafted packet. **CVE ID : CVE-2022-43109**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--221122/2766
Vendor: Fedoraproject					
Product: fedora					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 26					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	7.5	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on	https://www.openssl.org/news/secadv/20221101.txt, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0023, https://security.netapp.com/advisory/ntap-20221102-0001/	O-FED-FEDO-221122/2767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6). **CVE ID : CVE-2022-3602**		
Affected Version(s): 27					
Buffer Copy without Checking Size of Input	01-Nov-2022	7.5	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint	https://www.openssl.org/news/secadv/20221101.txt, https://psirt.global.sonicwal	O-FED-FEDO-221122/2768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue	l.com/vuln-detail/SNWLID-2022-0023, https://security.netapp.com/advisory/ntap-20221102-0001/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6). **CVE ID : CVE-2022-3602**		
Affected Version(s): 36					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	7.5	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the	https://www.openssl.org/news/secadv/20221101.txt, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0023, https://security.netapp.com/advisory/nta	O-FED-FEDO-221122/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded	p-20221102-0001/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6). **CVE ID : CVE-2022-3602**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	7.5	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker	https://www.openssl.org/news/secadv/20221101.txt	O-FED-FEDO-221122/2770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. **CVE ID : CVE-2022-3786**		
Affected Version(s): 37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	7.5	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the	https://www.openssl.org/news/secadv/20221101.txt, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0023, https://security.netapp.com/advisory/ntap-20221102-0001/	O-FED-FEDO-221122/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6). **CVE ID : CVE-2022-3602**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Nov-2022	7.5	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email	https://www.openssl.org/news/secadv/20221101.txt	O-FED-FEDO-221122/2772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address in a certificate to overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. **CVE ID : CVE-2022-3786**		
Improper Restriction of Rendered UI Layers or Frames	01-Nov-2022	6.1	The issue was addressed with improved UI handling. This issue is fixed in tvOS 16.1, macOS Ventura 13, watchOS 9.1, Safari 16.1, iOS 16.1 and iPadOS 16. Visiting a malicious website may lead to user interface spoofing. **CVE ID : CVE-2022-42799**	https://support.apple.com/en-us/HT213488, https://support.apple.com/en-us/HT213495, https://support.apple.com/en-us/HT213492, https://support.apple.com/en-	O-FED-FEDO-221122/2773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213491, https://support.apple.com/en-us/HT213489	
Vendor: Fortinet					
Product: fortios					
Affected Version(s): 6.4.9					
N/A	02-Nov-2022	8.1	A key management error vulnerability [CWE-320] affecting the RSA SSH host key in FortiOS 7.2.0 and below, 7.0.6 and below, 6.4.9 and below may allow an unauthenticated attacker to perform a man in the middle attack. **CVE ID : CVE-2022-30307**	https://fortiguard.com/psirt/FG-IR-22-228	O-FOR-FORT-221122/2774
Affected Version(s): 7.0.6					
N/A	02-Nov-2022	8.1	A key management error vulnerability [CWE-320] affecting the RSA SSH host key in FortiOS 7.2.0 and below, 7.0.6 and below, 6.4.9 and below may allow an unauthenticated attacker to perform a man in the middle attack. **CVE ID : CVE-2022-30307**	https://fortiguard.com/psirt/FG-IR-22-228	O-FOR-FORT-221122/2775
Affected Version(s): 7.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	O-FOR-FORT-221122/2776
N/A	02-Nov-2022	8.1	A key management error vulnerability [CWE-320] affecting the RSA SSH host key in FortiOS 7.2.0 and below, 7.0.6 and below, 6.4.9 and below may allow an unauthenticated attacker to perform a man in the middle attack. **CVE ID : CVE-2022-30307**	https://fortiguard.com/psirt/FG-IR-22-228	O-FOR-FORT-221122/2777
N/A	02-Nov-2022	7.5	An exposure of sensitive information to an unauthorized actor vulnerabiltiy [CWE-200] in FortiOS SSL-VPN versions 7.2.0, versions 7.0.0	https://fortiguard.com/psirt/FG-IR-22-223	O-FOR-FORT-221122/2778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 7.0.6 and versions 6.4.0 through 6.4.9 may allow a remote unauthenticated attacker to gain information about LDAP and SAML settings configured in FortiOS. **CVE ID : CVE-2022-35842**		
N/A	02-Nov-2022	4.3	An improper access control [CWE-284] vulnerability in FortiOS version 7.2.0 and versions 7.0.0 through 7.0.7 may allow a remote authenticated read-only user to modify the interface settings via the API. **CVE ID : CVE-2022-38380**	https://fortiguard.com/psirt/FG-IR-22-174	O-FOR-FORT-221122/2779
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.15					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad	https://fortiguard.com/psirt/FG-IR-22-074	O-FOR-FORT-221122/2780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			characters in base64. **CVE ID : CVE-2022-26122**		
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.11					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad characters in base64. **CVE ID : CVE-2022-26122**	https://fortiguard.com/psirt/FG-IR-22-074	O-FOR-FORT-221122/2781
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.10					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad	https://fortiguard.com/psirt/FG-IR-22-074	O-FOR-FORT-221122/2782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			characters in base64. **CVE ID : CVE-2022-26122**		
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.9					
N/A	02-Nov-2022	7.5	An exposure of sensitive information to an unauthorized actor vulnerabiltiy [CWE-200] in FortiOS SSL-VPN versions 7.2.0, versions 7.0.0 through 7.0.6 and versions 6.4.0 through 6.4.9 may allow a remote unauthenticated attacker to gain information about LDAP and SAML settings configured in FortiOS. **CVE ID : CVE-2022-35842**	https://fortiguard.com/psirt/FG-IR-22-223	O-FOR-FORT-221122/2783
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.6					
Insufficient Verification of Data Authenticity	02-Nov-2022	8.6	An insufficient verification of data authenticity vulnerability [CWE-345] in FortiClient, FortiMail and FortiOS AV engines version 6.2.168 and below and version 6.4.274 and below may allow an attacker to bypass the AV engine via manipulating MIME attachment with junk and pad	https://fortiguard.com/psirt/FG-IR-22-074	O-FOR-FORT-221122/2784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			characters in base64. **CVE ID : CVE-2022-26122**		
N/A	02-Nov-2022	7.5	An exposure of sensitive information to an unauthorized actor vulnerabiltiy [CWE-200] in FortiOS SSL-VPN versions 7.2.0, versions 7.0.0 through 7.0.6 and versions 6.4.0 through 6.4.9 may allow a remote unauthenticated attacker to gain information about LDAP and SAML settings configured in FortiOS. **CVE ID : CVE-2022-35842**	https://fortiguard.com/psirt/FG-IR-22-223	O-FOR-FORT-221122/2785
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.7					
N/A	02-Nov-2022	4.3	An improper access control [CWE-284] vulnerability in FortiOS version 7.2.0 and versions 7.0.0 through 7.0.7 may allow a remote authenticated read-only user to modify the interface settings via the API. **CVE ID : CVE-2022-38380**	https://fortiguard.com/psirt/FG-IR-22-174	O-FOR-FORT-221122/2786
Vendor: Freebsd					
Product: freebsd					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.5	Insufficient validation of the IOCTL input buffer in AMD ?Prof may allow an attacker to send an arbitrary buffer leading to a potential Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-23831**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	O-FRE-FREE-221122/2787
N/A	09-Nov-2022	7.5	Insufficient validation in the IOCTL input/output buffer in AMD ?Prof may allow an attacker to bypass bounds checks potentially leading to a Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-27674**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	O-FRE-FREE-221122/2788
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	01-Nov-2022	6.5	Insufficient policy enforcement in custom tabs in Google Chrome on Android prior to 106.0.5249.62 allowed an attacker who convinced the user to install an application to bypass same origin policy via a crafted	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html, https://crbug.com/1240065	O-GOO-ANDR-221122/2789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application. (Chromium security severity: Medium) **CVE ID : CVE-2022-3310**		
Improper Input Validation	01-Nov-2022	4.3	Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 106.0.5249.62 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2022-3317**	https://crbug.com/1300539, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	O-GOO-ANDR-221122/2790
N/A	09-Nov-2022	4.3	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 106.0.5249.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3447**	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html	O-GOO-ANDR-221122/2791
Improper Input Validation	01-Nov-2022	4.3	Inappropriate implementation in Full screen mode in	https://crbug.com/1327505,	O-GOO-ANDR-221122/2792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Google Chrome on Android prior to 107.0.5304.62 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2022-3660**	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html	
Affected Version(s): 10.0					
N/A	08-Nov-2022	7.8	In navigateUpTo of Task.java, there is a possible way to launch an unexported intent handler due to a logic error in the code. This could lead to local escalation of privilege if the targeted app has an intent trampoline, 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-238605611 **CVE ID : CVE-2022-20441**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	08-Nov-2022	7.8	In restorePermissionState of PermissionManagerServiceImpl.java, there is a possible way to bypass user consent due to a missing permission 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-10 Android-11 Android-12 Android-12L Android-13Android ID: A-210065877 **CVE ID : CVE-2022-20450**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2794
Missing Authorization	08-Nov-2022	7.8	In onCallRedirectionComplete of CallsManager.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235098883 **CVE ID : CVE-2022-20451**		
Out-of-bounds Write	08-Nov-2022	7.8	In phNxpNciHal_write_unlocked of phNxpNciHal.cc, 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 privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230356196 **CVE ID : CVE-2022-20462**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2796
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass due to a parcel format mismatch. This could lead to	https://corp.mediatek.com/product-security-	O-GOO-ANDR-221122/2797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	bulletin/November-2022	
Out-of-bounds Write	09-Nov-2022	7.8	Heap overflow vulnerability in sflacf_fal_bytes_peek function in libsmat.so library prior to SMR Nov-2022 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2022-39882**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2798
Incorrect Permission Assignment for Critical Resource	09-Nov-2022	7.8	Improper authorization vulnerability in StorageManagerService prior to SMR Nov-2022 Release 1 allows local attacker to call privileged API. **CVE ID : CVE-2022-39883**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2799
Out-of-bounds Read	08-Nov-2022	7.5	In process_service_search_rsp of sdp_discovery.cc, there is a possible out of bounds read	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper input validation. 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-225876506 **CVE ID : CVE-2022-20445**		
Integer Overflow or Wraparound	08-Nov-2022	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds write due to an integer overflow. 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-242096164 **CVE ID : CVE-2022-20454**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2802
Improper Check for Unusual or Exceptional Conditions	08-Nov-2022	5.5	In setImpl of AlarmManagerService.java, there is a possible way to put a device into a boot loop due to an uncaught exception. This could lead to local denial of service 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-234441463	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20414		
Uncontrolled Resource Consumption	08-Nov-2022	5.5	In multiple functions of many files, there is a possible obstruction of the user's ability to select a phone account due to resource exhaustion. This could lead to local denial of service 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-236263294 **CVE ID : CVE-2022-20426**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2804
N/A	08-Nov-2022	5.5	In buzzBeepBlinkLocked of NotificationManagerService.java, there is a possible way to share data across users due to a permissions bypass. This could lead to local escalation of privilege with no additional	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-237540408 **CVE ID : CVE-2022-20448**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	5.5	In update of MmsProvider.java, there is a possible constriction of directory permissions due to a path traversal error. This could lead to local denial of service of SIM recognition with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240685104 **CVE ID : CVE-2022-20453**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2806
N/A	08-Nov-2022	4.6	In dismiss and related functions of KeyguardHostView	https://source.android.com/security/bull	O-GOO-ANDR-221122/2807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller.java and related files, there is a possible lockscreen bypass 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-218500036 **CVE ID : CVE-2022-20465**	etin/2022-11-01	
Missing Authorization	08-Nov-2022	3.3	In AlwaysOnHotwordDetector of AlwaysOnHotwordDetector.java, there is a possible way to access the microphone from the background due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-229793943 **CVE ID : CVE-2022-20446**		
N/A	08-Nov-2022	3.3	In factoryReset of WifiServiceImpl, there is a possible way to preserve WiFi settings due to a logic error in the code. This could lead to a local non-security issue across network factory resets 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-231985227 **CVE ID : CVE-2022-20463**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2809
N/A	09-Nov-2022	3.3	Improper access control vulnerability in IImsService prior to SMR Nov-2022 Release 1 allows local attacker to access to Call information.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39884		
N/A	09-Nov-2022	3.3	Improper access control vulnerability in BootCompletedReceiver_CMCC in DeviceManagement prior to SMR Nov-2022 Release 1 allows local attacker to access to Device information. **CVE ID : CVE-2022-39885**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2811
Exposure of Resource to Wrong Sphere	09-Nov-2022	3.3	Improper access control vulnerability in IpcRxServiceModeBigDataInfo in RIL prior to SMR Nov-2022 Release 1 allows local attacker to access Device information. **CVE ID : CVE-2022-39886**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2812
Incorrect Permission Assignment for Critical Resource	09-Nov-2022	3.3	Improper access control vulnerability in clearAllGlobalProxy in MiscPolicy prior to SMR Nov-2022 Release 1 allows local attacker to configure EDM setting. **CVE ID : CVE-2022-39887**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2813
Affected Version(s): 11.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Nov-2022	7.8	In navigateUpTo of Task.java, there is a possible way to launch an unexported intent handler due to a logic error in the code. This could lead to local escalation of privilege if the targeted app has an intent trampoline, 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-238605611 **CVE ID : CVE-2022-20441**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2814
Missing Authorization	08-Nov-2022	7.8	In restorePermissionState of PermissionManagerServiceImpl.java, there is a possible way to bypass user consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-210065877 **CVE ID : CVE-2022-20450**		
Missing Authorization	08-Nov-2022	7.8	In onCallRedirectionComplete of CallsManager.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235098883 **CVE ID : CVE-2022-20451**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2816
Out-of-bounds Write	08-Nov-2022	7.8	In phNxpNciHal_write_unlocked of phNxpNciHal.cc,	https://source.android.com/security/bull	O-GOO-ANDR-221122/2817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230356196 **CVE ID : CVE-2022-20462**	etin/2022-11-01	
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-Nov-2022	7.8	Improper input validation vulnerability in DualOutFocusViewer prior to SMR Nov-2022 Release 1 allows local attacker to perform an arbitrary code execution. **CVE ID : CVE-2022-39880**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2819
Out-of-bounds Write	09-Nov-2022	7.8	Heap overflow vulnerability in sflacf_fal_bytes_peek function in libsmat.so library prior to SMR Nov-2022 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2022-39882**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2820
Incorrect Permission Assignment for Critical Resource	09-Nov-2022	7.8	Improper authorization vulnerability in StorageManagerService prior to SMR Nov-2022 Release 1 allows local attacker to call privileged API. **CVE ID : CVE-2022-39883**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2821
Out-of-bounds Read	08-Nov-2022	7.5	In process_service_search_rsp of sdp_discovery.cc, there is a possible out of bounds read due to improper	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. 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-225876506 **CVE ID : CVE-2022-20445**		
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262364; Issue ID: ALPS07262364. **CVE ID : CVE-2022-32617**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262454; Issue ID: ALPS07262454. **CVE ID : CVE-2022-32618**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2824
Integer Overflow or Wraparound	08-Nov-2022	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds write due to an integer overflow. 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-242096164	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20454		
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2826
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891; Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2827
Out-of-bounds Write	08-Nov-2022	6.7	In isp, there is a possible out of bounds write due	https://corp.mediatek.com/product-	O-GOO-ANDR-221122/2828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07340373; Issue ID: ALPS07340373. **CVE ID : CVE-2022-32611**	security-bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2829
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. 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/November-2022	O-GOO-ANDR-221122/2830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2831
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2832
Improper Check for	08-Nov-2022	5.5	In setImpl of AlarmManagerServ	https://source.android.com	O-GOO-ANDR-221122/2833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			ice.java, there is a possible way to put a device into a boot loop due to an uncaught exception. This could lead to local denial of service 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-234441463 **CVE ID : CVE-2022-20414**	/security/bulletin/2022-11-01	
Uncontrolled Resource Consumption	08-Nov-2022	5.5	In multiple functions of many files, there is a possible obstruction of the user's ability to select a phone account due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12L Android-13Android ID: A-236263294 **CVE ID : CVE-2022-20426**		
N/A	08-Nov-2022	5.5	In buzzBeepBlinkLocked of NotificationManagerService.java, there is a possible way to share data across users due to a permissions bypass. 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-237540408 **CVE ID : CVE-2022-20448**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2835
Improper Limitation of a Pathname to a Restricted Directory	08-Nov-2022	5.5	In update of MmsProvider.java, there is a possible constriction of directory permissions due to a path traversal error. This could	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			lead to local denial of service of SIM recognition with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240685104 **CVE ID : CVE-2022-20453**		
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2837
N/A	08-Nov-2022	4.6	In dismiss and related functions of KeyguardHostViewController.java and related files, there is a possible	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lockscreen bypass 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-218500036 **CVE ID : CVE-2022-20465**		
Missing Authorization	08-Nov-2022	3.3	In AlwaysOnHotwordDetector of AlwaysOnHotwordDetector.java, there is a possible way to access the microphone from the background due to a missing permission 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-10	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11Android ID: A-229793943 **CVE ID : CVE-2022-20446**		
N/A	08-Nov-2022	3.3	In factoryReset of WifiServiceImpl, there is a possible way to preserve WiFi settings due to a logic error in the code. This could lead to a local non-security issue across network factory resets 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-231985227 **CVE ID : CVE-2022-20463**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2840
Missing Authorization	09-Nov-2022	3.3	Improper authorization vulnerability in?CallBGProvider prior to SMR Nov-2022 Release 1 allows local attacker to grant permission for accessing information with phone uid.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39879		
N/A	09-Nov-2022	3.3	Improper access control vulnerability in IImsService prior to SMR Nov-2022 Release 1 allows local attacker to access to Call information. **CVE ID : CVE-2022-39884**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2842
N/A	09-Nov-2022	3.3	Improper access control vulnerability in BootCompletedReceiver_CMCC in DeviceManagement prior to SMR Nov-2022 Release 1 allows local attacker to access to Device information. **CVE ID : CVE-2022-39885**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2843
Exposure of Resource to Wrong Sphere	09-Nov-2022	3.3	Improper access control vulnerability in IpcRxServiceModeBigDataInfo in RIL prior to SMR Nov-2022 Release 1 allows local attacker to access Device information. **CVE ID : CVE-2022-39886**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2844
Incorrect Permission Assignmen	09-Nov-2022	3.3	Improper access control vulnerability in	https://security.samsungmobile.com/secu	O-GOO-ANDR-221122/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t for Critical Resource			clearAllGlobalProxy in MiscPolicy prior to SMR Nov-2022 Release 1 allows local attacker to configure EDM setting. **CVE ID : CVE-2022-39887**	rityUpdate.smsb?year=2022&month=11	
Affected Version(s): 12.0					
N/A	08-Nov-2022	7.8	In navigateUpTo of Task.java, there is a possible way to launch an unexported intent handler due to a logic error in the code. This could lead to local escalation of privilege if the targeted app has an intent trampoline, 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-238605611 **CVE ID : CVE-2022-20441**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2846
Missing Authorization	08-Nov-2022	7.8	In restorePermissionState of PermissionManage	https://source.android.com/security/bull	O-GOO-ANDR-221122/2847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rServiceImpl.java, there is a possible way to bypass user consent due to a missing permission 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-10 Android-11 Android-12 Android-12L Android-13Android ID: A-210065877 **CVE ID : CVE-2022-20450**	etin/2022-11-01	
Missing Authorization	08-Nov-2022	7.8	In onCallRedirectionComplete of CallsManager.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12L Android-13Android ID: A-235098883 **CVE ID : CVE-2022-20451**		
Out-of-bounds Write	08-Nov-2022	7.8	In phNxpNciHal_write_unlocked of phNxpNciHal.cc, 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 privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230356196 **CVE ID : CVE-2022-20462**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2849
Deserialization of Untrusted Data	08-Nov-2022	7.8	In telephony, there is a possible permission bypass 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/November-2022	O-GOO-ANDR-221122/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07319132; Issue ID: ALPS07319132. **CVE ID : CVE-2022-32601**		
Improper Input Validation	09-Nov-2022	7.8	Improper input validation vulnerability in DualOutFocusViewer prior to SMR Nov-2022 Release 1 allows local attacker to perform an arbitrary code execution. **CVE ID : CVE-2022-39880**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2851
Out-of-bounds Write	09-Nov-2022	7.8	Heap overflow vulnerability in sflacf_fal_bytes_peek function in libsmat.so library prior to SMR Nov-2022 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2022-39882**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2852
Incorrect Permission Assignment for Critical Resource	09-Nov-2022	7.8	Improper authorization vulnerability in StorageManagerService prior to SMR Nov-2022 Release 1 allows local attacker to call privileged API.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39883		
Out-of-bounds Read	08-Nov-2022	7.5	In process_service_search_rsp of sdp_discovery.cc, there is a possible out of bounds read due to improper input validation. 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-225876506 **CVE ID : CVE-2022-20445**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2854
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07262364; Issue ID: ALPS07262364. **CVE ID : CVE-2022-32617**		
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262454; Issue ID: ALPS07262454. **CVE ID : CVE-2022-32618**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2856
Use After Free	08-Nov-2022	6.7	In aee, there is a possible use after free 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: ALPS07202891;	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07202891. **CVE ID : CVE-2022-32607**		
Improper Input Validation	08-Nov-2022	6.7	In gpu drm, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310704; Issue ID: ALPS07310704. **CVE ID : CVE-2022-32603**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2858
Out-of-bounds Write	08-Nov-2022	6.7	In isp, there is a possible out of bounds write 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. Patch ID: ALPS07213898; Issue ID: ALPS07213898. **CVE ID : CVE-2022-32605**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2859
Integer Overflow	08-Nov-2022	6.7	In fdt_next_tag of fdt.c, there is a	https://source.android.com	O-GOO-ANDR-221122/2860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			possible out of bounds write due to an integer overflow. 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-242096164 **CVE ID : CVE-2022-20454**	/security/bulletin/2022-11-01	
Out-of-bounds Read	08-Nov-2022	6.7	In vpu, there is a possible information disclosure 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. Patch ID: ALPS06382421; Issue ID: ALPS06382421. **CVE ID : CVE-2022-21778**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Nov-2022	6.7	In isp, 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: ALPS07340373; Issue ID: ALPS07340373. **CVE ID : CVE-2022-32611**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2862
Double Free	08-Nov-2022	6.7	In audio, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310571; Issue ID: ALPS07310571. **CVE ID : CVE-2022-32614**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2863
Improper Input Validation	08-Nov-2022	6.7	In ccd, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326559; Issue ID: ALPS07326559. **CVE ID : CVE-2022-32615**		
Improper Input Validation	08-Nov-2022	6.7	In isp, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07341258; Issue ID: ALPS07341258. **CVE ID : CVE-2022-32616**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2865
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Nov-2022	6.4	In jpeg, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388753;	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07388753. **CVE ID : CVE-2022-32608**		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2867
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410. **CVE ID : CVE-2022-32609**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2868
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This	https://corp.mediatek.com/product-security-	O-GOO-ANDR-221122/2869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	bulletin/November-2022	
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2870
N/A	08-Nov-2022	5.5	In buzzBeepBlinkLocked of NotificationManagerService.java, there is a possible way to share data across users due to a permissions bypass. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-237540408 **CVE ID : CVE-2022-20448**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	5.5	In update of MmsProvider.java, there is a possible constriction of directory permissions due to a path traversal error. This could lead to local denial of service of SIM recognition with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240685104 **CVE ID : CVE-2022-20453**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	5.5	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388790; Issue ID: ALPS07388790. **CVE ID : CVE-2022-32602**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2873
Improper Check for Unusual or Exceptional Conditions	08-Nov-2022	5.5	In setImpl of AlarmManagerService.java, there is a possible way to put a device into a boot loop due to an uncaught exception. This could lead to local denial of service 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-234441463	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20414		
Uncontrolled Resource Consumption	08-Nov-2022	5.5	In multiple functions of many files, there is a possible obstruction of the user's ability to select a phone account due to resource exhaustion. This could lead to local denial of service 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-236263294 **CVE ID : CVE-2022-20426**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2875
N/A	08-Nov-2022	4.6	In dismiss and related functions of KeyguardHostViewController.java and related files, there is a possible lockscreen bypass 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/2022-11-01	O-GOO-ANDR-221122/2876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-218500036 **CVE ID : CVE-2022-20465**		
N/A	08-Nov-2022	3.3	In factoryReset of WifiServiceImpl, there is a possible way to preserve WiFi settings due to a logic error in the code. This could lead to a local non-security issue across network factory resets 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-231985227 **CVE ID : CVE-2022-20463**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2877
Missing Authorization	09-Nov-2022	3.3	Improper authorization vulnerability in?CallBGProvider	https://security.samsungmobile.com/securityUpdate.sm	O-GOO-ANDR-221122/2878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to SMR Nov-2022 Release 1 allows local attacker to grant permission for accessing information with phone uid. **CVE ID : CVE-2022-39879**	sb?year=2022&month=11	
N/A	09-Nov-2022	3.3	Improper access control vulnerability in IImsService prior to SMR Nov-2022 Release 1 allows local attacker to access to Call information. **CVE ID : CVE-2022-39884**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2879
N/A	09-Nov-2022	3.3	Improper access control vulnerability in BootCompletedReceiver_CMCC in DeviceManagement prior to SMR Nov-2022 Release 1 allows local attacker to access to Device information. **CVE ID : CVE-2022-39885**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2880
Exposure of Resource to Wrong Sphere	09-Nov-2022	3.3	Improper access control vulnerability in IpcRxServiceModeBigDataInfo in RIL prior to SMR Nov-2022 Release 1	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows local attacker to access Device information. **CVE ID : CVE-2022-39886**		
Incorrect Permission Assignment for Critical Resource	09-Nov-2022	3.3	Improper access control vulnerability in clearAllGlobalProxy in MiscPolicy prior to SMR Nov-2022 Release 1 allows local attacker to configure EDM setting. **CVE ID : CVE-2022-39887**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-GOO-ANDR-221122/2882
Affected Version(s): 12.1					
N/A	08-Nov-2022	7.8	In navigateUpTo of Task.java, there is a possible way to launch an unexported intent handler due to a logic error in the code. This could lead to local escalation of privilege if the targeted app has an intent trampoline, 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/2022-11-01	O-GOO-ANDR-221122/2883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-238605611 **CVE ID : CVE-2022-20441**		
Missing Authorization	08-Nov-2022	7.8	In restorePermissionState of PermissionManagerServiceImpl.java, there is a possible way to bypass user consent due to a missing permission 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-10 Android-11 Android-12 Android-12L Android-13Android ID: A-210065877 **CVE ID : CVE-2022-20450**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2884
Missing Authorization	08-Nov-2022	7.8	In onCallRedirectionComplete of CallsManager.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235098883 **CVE ID : CVE-2022-20451**		
Out-of-bounds Write	08-Nov-2022	7.8	In phNxpNciHal_write_unlocked of phNxpNciHal.cc, 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 privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230356196 **CVE ID : CVE-2022-20462**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	7.5	In process_service_search_rsp of sdp_discovery.cc, there is a possible out of bounds read due to improper input validation. 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-225876506 **CVE ID : CVE-2022-20445**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2887
Integer Overflow or Wraparound	08-Nov-2022	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds write due to an integer overflow. 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	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12 Android-12L Android-13Android ID: A-242096164 **CVE ID : CVE-2022-20454**		
Improper Check for Unusual or Exceptional Conditions	08-Nov-2022	5.5	In setImpl of AlarmManagerService.java, there is a possible way to put a device into a boot loop due to an uncaught exception. This could lead to local denial of service 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-234441463 **CVE ID : CVE-2022-20414**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2889
Uncontrolled Resource Consumption	08-Nov-2022	5.5	In multiple functions of many files, there is a possible obstruction of the user's ability to select a phone account due to resource exhaustion. This could lead to local denial of service	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-236263294 **CVE ID : CVE-2022-20426**		
N/A	08-Nov-2022	5.5	In buzzBeepBlinkLocked of NotificationManagerService.java, there is a possible way to share data across users due to a permissions bypass. 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-237540408 **CVE ID : CVE-2022-20448**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	5.5	In update of MmsProvider.java, there is a possible constriction of directory permissions due to a path traversal error. This could lead to local denial of service of SIM recognition with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240685104 **CVE ID : CVE-2022-20453**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2892
N/A	08-Nov-2022	4.6	In dismiss and related functions of KeyguardHostViewController.java and related files, there is a possible lockscreen bypass 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	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2893

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-218500036 **CVE ID : CVE-2022-20465**		
N/A	08-Nov-2022	3.3	In factoryReset of WifiServiceImpl, there is a possible way to preserve WiFi settings due to a logic error in the code. This could lead to a local non-security issue across network factory resets 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-231985227 **CVE ID : CVE-2022-20463**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2894
Affected Version(s): 13.0					
N/A	08-Nov-2022	7.8	In navigateUpTo of Task.java, there is a possible way to launch an unexported intent	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handler due to a logic error in the code. This could lead to local escalation of privilege if the targeted app has an intent trampoline, 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-238605611 **CVE ID : CVE-2022-20441**		
Missing Authorization	08-Nov-2022	7.8	In restorePermissionState of PermissionManagerServiceImpl.java, there is a possible way to bypass user consent due to a missing permission check. 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/2022-11-01	O-GOO-ANDR-221122/2896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-210065877 **CVE ID : CVE-2022-20450**		
Missing Authorization	08-Nov-2022	7.8	In onCallRedirectionComplete of CallsManager.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-235098883 **CVE ID : CVE-2022-20451**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2897
N/A	08-Nov-2022	7.8	In initializeFromParcelLocked of BaseBundle.java, there is a possible method arbitrary code execution due to a confused deputy. This could	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-240138318 **CVE ID : CVE-2022-20452**		
Out-of-bounds Write	08-Nov-2022	7.8	In phNxpNciHal_write_unlocked of phNxpNciHal.cc, 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 privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230356196 **CVE ID : CVE-2022-20462**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Nov-2022	7.5	In process_service_search_rsp of sdp_discovery.cc, there is a possible out of bounds read due to improper input validation. 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-225876506 **CVE ID : CVE-2022-20445**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2900
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07262364; Issue ID: ALPS07262364. **CVE ID : CVE-2022-32617**		
Incorrect Calculation of Buffer Size	08-Nov-2022	6.8	In typec, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262454; Issue ID: ALPS07262454. **CVE ID : CVE-2022-32618**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2902
Integer Overflow or Wraparound	08-Nov-2022	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12L Android-13Android ID: A-242096164 **CVE ID : CVE-2022-20454**		
Use After Free	08-Nov-2022	6.5	In PAN_WriteBuf of pan_api.cc, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233604485 **CVE ID : CVE-2022-20447**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2904
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203410; Issue ID: ALPS07203410.	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32609		
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203476; Issue ID: ALPS07203476. **CVE ID : CVE-2022-32610**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2906
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203500; Issue ID: ALPS07203500. **CVE ID : CVE-2022-32612**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2907
Improper Synchronization	08-Nov-2022	6.4	In vcu, there is a possible memory corruption due to a race condition. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/November-2022	O-GOO-ANDR-221122/2908

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: ALPS07206340; Issue ID: ALPS07206340. **CVE ID : CVE-2022-32613**		
Improper Check for Unusual or Exceptional Conditions	08-Nov-2022	5.5	In setImpl of AlarmManagerService.java, there is a possible way to put a device into a boot loop due to an uncaught exception. This could lead to local denial of service 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-234441463 **CVE ID : CVE-2022-20414**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2909
Uncontrolled Resource Consumption	08-Nov-2022	5.5	In multiple functions of many files, there is a possible obstruction of the user's ability to select a phone	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account due to resource exhaustion. This could lead to local denial of service 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-236263294 **CVE ID : CVE-2022-20426**		
N/A	08-Nov-2022	5.5	In buzzBeepBlinkLocked of NotificationManagerService.java, there is a possible way to share data across users due to a permissions bypass. 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	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12L Android-13Android ID: A-237540408 **CVE ID : CVE-2022-20448**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Nov-2022	5.5	In update of MmsProvider.java, there is a possible constriction of directory permissions due to a path traversal error. This could lead to local denial of service of SIM recognition with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240685104 **CVE ID : CVE-2022-20453**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2912
Improper Input Validation	08-Nov-2022	5.5	In getMountModeInternal of StorageManagerService.java, there is a possible prevention of package installation due to improper input validation. This could lead to local escalation of	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-243924784 **CVE ID : CVE-2022-20457**		
N/A	08-Nov-2022	4.6	In dismiss and related functions of KeyguardHostViewController.java and related files, there is a possible lockscreen bypass 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-218500036 **CVE ID : CVE-2022-20465**	https://source.android.com/security/bulletin/2022-11-01	O-GOO-ANDR-221122/2914
N/A	08-Nov-2022	3.3	In factoryReset of WifiServiceImpl, there is a possible way to preserve	https://source.android.com/security/bull	O-GOO-ANDR-221122/2915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WiFi settings due to a logic error in the code. This could lead to a local non-security issue across network factory resets 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-231985227 **CVE ID : CVE-2022-20463**	etin/2022-11-01	
Product: chrome_os					
Affected Version(s): -					
Use After Free	01-Nov-2022	8.8	Use after free in survey in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3305**	https://crbug.com/1319229, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	O-GOO-CHRO-221122/2916
Use After Free	01-Nov-2022	8.8	Use after free in survey in Google Chrome on	https://crbug.com/1320139,	O-GOO-CHRO-221122/2917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ChromeOS prior to 106.0.5249.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-3306**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	
Use After Free	01-Nov-2022	8.8	Use after free in Feedback service on Chrome OS in Google Chrome on Chrome OS prior to 107.0.5304.62 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2022-3658**	https://crbug.com/1352817, https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html	O-GOO-CHRO-221122/2918
Use After Free	01-Nov-2022	8.8	Use after free in Accessibility in Google Chrome on Chrome OS prior to 107.0.5304.62 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit	https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html, https://crbug.com/1355560	O-GOO-CHRO-221122/2919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap corruption via specific UI interactions. (Chromium security severity: Medium) **CVE ID : CVE-2022-3659**		
Use After Free	01-Nov-2022	6.5	Use after free in assistant in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via specific UI gestures. (Chromium security severity: Medium) **CVE ID : CVE-2022-3309**	https://crbug.com/1348415, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html	O-GOO-CHRO-221122/2920
Use After Free	01-Nov-2022	6.5	Use after free in ChromeOS Notifications in Google Chrome on ChromeOS prior to 106.0.5249.62 allowed a remote attacker who convinced a user to reboot Chrome OS to potentially exploit heap corruption via UI interaction. (Chromium	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html, https://crbug.com/1318791	O-GOO-CHRO-221122/2921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Low) **CVE ID : CVE-2022-3318**		
Vendor: HP					
Product: hp-ux					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/support/pages/node/6833806	O-HP-HP-U-221122/2922
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**	https://www.ibm.com/support/pages/node/6829907	O-HP-HP-U-221122/2923
Improper Neutralization of Input During Web Page	11-Nov-2022	5.4	IBM WebSphere Application Server 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows	https://exchange.xforce.ibmcloud.com/vulnerabilities/236588, https://www.i	O-HP-HP-U-221122/2924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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: 236588. **CVE ID : CVE-2022-40750**	bm.com/support/pages/node/6833552	
Vendor: Huawei					
Product: emui					
Affected Version(s): 12.0					
N/A	09-Nov-2022	7.5	The kernel module has the vulnerability that the mapping is not cleared after the memory is automatically released. Successful exploitation of this vulnerability may cause a system restart. **CVE ID : CVE-2022-44546**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2925
Use After Free	09-Nov-2022	7.5	The Display Service module has a UAF vulnerability. Successful exploitation of this vulnerability may affect the display service availability.	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-	O-HUA-EMUI-221122/2926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44547	bulletins-phones-202211-0000001441016433	
Affected Version(s): 11.0.1					
N/A	09-Nov-2022	9.8	The iaware module has a vulnerability in thread security. Successful exploitation of this vulnerability will affect confidentiality, integrity, and availability. **CVE ID : CVE-2022-44551**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2927
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44558**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2928
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.co	O-HUA-EMUI-221122/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44559**	m/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	
Improper Privilege Management	09-Nov-2022	9.8	The system framework layer has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44562**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2930
Exposure of Resource to Wrong Sphere	09-Nov-2022	7.5	The LBS module has a vulnerability in geofencing API access. Successful exploitation of this vulnerability may cause third-party apps to access the geofencing APIs without authorization, affecting user confidentiality. **CVE ID : CVE-2022-44549**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2931
N/A	09-Nov-2022	7.5	The graphics display module has a UAF vulnerability when traversing graphic layers.	https://consumer.huawei.com/en/support/bulletin/2022/11/,	O-HUA-EMUI-221122/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-44550**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	
N/A	09-Nov-2022	7.5	The lock screen module has defects introduced in the design process. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-44552**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2933
N/A	09-Nov-2022	7.5	The DDMP/ODMF module has a service hijacking vulnerability. Successful exploit of this vulnerability may cause services to be unavailable. **CVE ID : CVE-2022-44555**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2934
N/A	09-Nov-2022	7.5	The SmartTrimProcess Event module has a	https://consumer.huawei.com/en/support	O-HUA-EMUI-221122/2935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability of obtaining the read and write permissions on arbitrary system files. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-44557**	/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	There is a race condition vulnerability in SD upgrade mode. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-44563**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2936
N/A	09-Nov-2022	5.3	The HiView module has a vulnerability of not filtering third-party apps out when the HiView module traverses to invoke the system provider. Successful exploitation of this vulnerability may cause third-party apps to start periodically.	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44553		
Incorrect Default Permissions	09-Nov-2022	4.3	There is a vulnerability in permission verification during the Bluetooth pairing process. Successful exploitation of this vulnerability may cause the dialog box for confirming the pairing not to be displayed during Bluetooth pairing. **CVE ID : CVE-2022-44548**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2938
Affected Version(s): 12.0.0					
N/A	09-Nov-2022	9.8	The iaware module has a vulnerability in thread security. Successful exploitation of this vulnerability will affect confidentiality, integrity, and availability. **CVE ID : CVE-2022-44551**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2939
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/se	O-HUA-EMUI-221122/2940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause privilege escalation. **CVE ID : CVE-2022-44558**	curity/update/security-bulletins-phones-202211-00000014410 16433	
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44559**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2941
Improper Privilege Management	09-Nov-2022	9.8	The system framework layer has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44562**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2942
Exposure of Resource to Wrong Sphere	09-Nov-2022	7.5	The LBS module has a vulnerability in geofencing API access. Successful exploitation of this vulnerability may	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device	O-HUA-EMUI-221122/2943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause third-party apps to access the geofencing APIs without authorization, affecting user confidentiality. **CVE ID : CVE-2022-44549**	.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	
N/A	09-Nov-2022	7.5	The graphics display module has a UAF vulnerability when traversing graphic layers. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-44550**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2944
N/A	09-Nov-2022	7.5	The power module has a vulnerability in permission verification. Successful exploitation of this vulnerability may cause abnormal status of a module on the device. **CVE ID : CVE-2022-44554**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2945
N/A	09-Nov-2022	7.5	The DDMP/ODMF module has a service hijacking vulnerability.	https://consumer.huawei.com/en/support/bulletin/202	O-HUA-EMUI-221122/2946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploit of this vulnerability may cause services to be unavailable. **CVE ID : CVE-2022-44555**	2/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	
Improper Input Validation	08-Nov-2022	7.5	Missing parameter type validation in the DRM module. Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2022-44556**	https://consumer.huawei.com/en/support/bulletin/2022/11/	O-HUA-EMUI-221122/2947
N/A	09-Nov-2022	7.5	The SmartTrimProcessEvent module has a vulnerability of obtaining the read and write permissions on arbitrary system files. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-44557**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2948
Concurrent Execution using Shared Resource with Improper	09-Nov-2022	5.9	There is a race condition vulnerability in SD upgrade mode. Successful exploitation of this vulnerability may	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.co	O-HUA-EMUI-221122/2949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			affect data confidentiality. **CVE ID : CVE-2022-44563**	m/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	
N/A	09-Nov-2022	5.3	The HiView module has a vulnerability of not filtering third-party apps out when the HiView module traverses to invoke the system provider. Successful exploitation of this vulnerability may cause third-party apps to start periodically. **CVE ID : CVE-2022-44553**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2950
Incorrect Default Permissions	09-Nov-2022	4.3	There is a vulnerability in permission verification during the Bluetooth pairing process. Successful exploitation of this vulnerability may cause the dialog box for confirming the pairing not to be displayed during Bluetooth pairing. **CVE ID : CVE-2022-44548**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2951
Affected Version(s): 12.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	9.8	The iaware module has a vulnerability in thread security. Successful exploitation of this vulnerability will affect confidentiality, integrity, and availability. **CVE ID : CVE-2022-44551**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2952
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44558**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-EMUI-221122/2953
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44559**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-	O-HUA-EMUI-221122/2954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				00000014410 16433	
Improper Privilege Manageme nt	09-Nov-2022	9.8	The system framework layer has a vulnerability of serialization/deseri alization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44562**	https://consu mer.huawei.co m/en/support /bulletin/202 2/11/, https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2955
Exposure of Resource to Wrong Sphere	09-Nov-2022	7.5	The LBS module has a vulnerability in geofencing API access. Successful exploitation of this vulnerability may cause third-party apps to access the geofencing APIs without authorization, affecting user confidentiality. **CVE ID : CVE-2022-44549**	https://consu mer.huawei.co m/en/support /bulletin/202 2/11/, https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2956
N/A	09-Nov-2022	7.5	The graphics display module has a UAF vulnerability when traversing graphic layers. Successful exploitation of this vulnerability may affect system availability.	https://consu mer.huawei.co m/en/support /bulletin/202 2/11/, https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-	O-HUA-EMUI-221122/2957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44550	phones-202211-00000014410 16433	
N/A	09-Nov-2022	7.5	The DDMP/ODMF module has a service hijacking vulnerability. Successful exploit of this vulnerability may cause services to be unavailable. **CVE ID : CVE-2022-44555**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2958
N/A	09-Nov-2022	7.5	The SmartTrimProcess Event module has a vulnerability of obtaining the read and write permissions on arbitrary system files. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-44557**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2959
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	5.9	There is a race condition vulnerability in SD upgrade mode. Successful exploitation of this vulnerability may	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update	O-HUA-EMUI-221122/2960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			affect data confidentiality. **CVE ID : CVE-2022-44563**	/security-bulletins-phones-202211-00000014410 16433	
N/A	09-Nov-2022	5.3	The HiView module has a vulnerability of not filtering third-party apps out when the HiView module traverses to invoke the system provider. Successful exploitation of this vulnerability may cause third-party apps to start periodically. **CVE ID : CVE-2022-44553**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2961
Incorrect Default Permissions	09-Nov-2022	4.3	There is a vulnerability in permission verification during the Bluetooth pairing process. Successful exploitation of this vulnerability may cause the dialog box for confirming the pairing not to be displayed during Bluetooth pairing. **CVE ID : CVE-2022-44548**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-EMUI-221122/2962
Product: harmonyos					
Affected Version(s): 2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	9.8	The iaware module has a vulnerability in thread security. Successful exploitation of this vulnerability will affect confidentiality, integrity, and availability. **CVE ID : CVE-2022-44551**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-HARM-221122/2963
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44558**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-HARM-221122/2964
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44559**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-	O-HUA-HARM-221122/2965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				00000014410 16433	
Improper Privilege Manageme nt	09-Nov-2022	9.8	The system framework layer has a vulnerability of serialization/deseri alization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44562**	https://consu mer.huawei.co m/en/support /bulletin/202 2/11/, https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2966
N/A	09-Nov-2022	7.5	The kernel module has the vulnerability that the mapping is not cleared after the memory is automatically released. Successful exploitation of this vulnerability may cause a system restart. **CVE ID : CVE-2022-44546**	https://consu mer.huawei.co m/en/support /bulletin/202 2/11/, https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2967
Use After Free	09-Nov-2022	7.5	The Display Service module has a UAF vulnerability. Successful exploitation of this vulnerability may affect the display service availability. **CVE ID : CVE-2022-44547**	https://consu mer.huawei.co m/en/support /bulletin/202 2/11/, https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-	O-HUA-HARM-221122/2968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				phones-202211-00000014410 16433	
Exposure of Resource to Wrong Sphere	09-Nov-2022	7.5	The LBS module has a vulnerability in geofencing API access. Successful exploitation of this vulnerability may cause third-party apps to access the geofencing APIs without authorization, affecting user confidentiality. **CVE ID : CVE-2022-44549**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2969
N/A	09-Nov-2022	7.5	The graphics display module has a UAF vulnerability when traversing graphic layers. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-44550**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2970
N/A	09-Nov-2022	7.5	The lock screen module has defects introduced in the design process. Successful exploitation of this vulnerability may	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update	O-HUA-HARM-221122/2971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect system availability. **CVE ID : CVE-2022-44552**	/security-bulletins-phones-202211-00000014410 16433	
N/A	09-Nov-2022	7.5	The power module has a vulnerability in permission verification. Successful exploitation of this vulnerability may cause abnormal status of a module on the device. **CVE ID : CVE-2022-44554**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2972
N/A	09-Nov-2022	7.5	The DDMP/ODMF module has a service hijacking vulnerability. Successful exploit of this vulnerability may cause services to be unavailable. **CVE ID : CVE-2022-44555**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2973
N/A	09-Nov-2022	7.5	The SmartTrimProcess Event module has a vulnerability of obtaining the read and write permissions on	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.co	O-HUA-HARM-221122/2974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary system files. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-44557**	m/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	There is a race condition vulnerability in SD upgrade mode. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-44563**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2975
N/A	09-Nov-2022	5.3	The HiView module has a vulnerability of not filtering third-party apps out when the HiView module traverses to invoke the system provider. Successful exploitation of this vulnerability may cause third-party apps to start periodically. **CVE ID : CVE-2022-44553**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2976
Incorrect Default	09-Nov-2022	4.3	There is a vulnerability in	https://consumer.huawei.co	O-HUA-HARM-221122/2977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			permission verification during the Bluetooth pairing process. Successful exploitation of this vulnerability may cause the dialog box for confirming the pairing not to be displayed during Bluetooth pairing. **CVE ID : CVE-2022-44548**	m/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	
Affected Version(s): 2.1					
N/A	09-Nov-2022	9.8	The iaware module has a vulnerability in thread security. Successful exploitation of this vulnerability will affect confidentiality, integrity, and availability. **CVE ID : CVE-2022-44551**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-0000001441016433	O-HUA-HARM-221122/2978
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44558**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-	O-HUA-HARM-221122/2979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				00000014410 16433	
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44559**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2980
Improper Privilege Management	09-Nov-2022	9.8	The system framework layer has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44562**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2981
Exposure of Resource to Wrong Sphere	09-Nov-2022	7.5	The LBS module has a vulnerability in geofencing API access. Successful exploitation of this vulnerability may cause third-party apps to access the geofencing APIs without authorization,	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-HARM-221122/2982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affecting user confidentiality. **CVE ID : CVE-2022-44549**	phones-202211-00000014410 16433	
N/A	09-Nov-2022	7.5	The graphics display module has a UAF vulnerability when traversing graphic layers. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-44550**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2983
N/A	09-Nov-2022	7.5	The DDMP/ODMF module has a service hijacking vulnerability. Successful exploit of this vulnerability may cause services to be unavailable. **CVE ID : CVE-2022-44555**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2984
N/A	09-Nov-2022	7.5	The SmartTrimProcess Event module has a vulnerability of obtaining the read and write permissions on arbitrary system files. Successful	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update	O-HUA-HARM-221122/2985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-44557**	/security-bulletins-phones-202211-00000014410 16433	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	There is a race condition vulnerability in SD upgrade mode. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-44563**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2986
N/A	09-Nov-2022	5.3	The HiView module has a vulnerability of not filtering third-party apps out when the HiView module traverses to invoke the system provider. Successful exploitation of this vulnerability may cause third-party apps to start periodically. **CVE ID : CVE-2022-44553**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2987
Incorrect Default Permissions	09-Nov-2022	4.3	There is a vulnerability in permission verification during	https://consumer.huawei.com/en/support/bulletin/202	O-HUA-HARM-221122/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Bluetooth pairing process. Successful exploitation of this vulnerability may cause the dialog box for confirming the pairing not to be displayed during Bluetooth pairing. **CVE ID : CVE-2022-44548**	2/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	
Affected Version(s): 3.0.0					
Deserialization of Untrusted Data	09-Nov-2022	9.8	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44559**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2989
Improper Privilege Management	09-Nov-2022	9.8	The system framework layer has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-44562**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-	O-HUA-HARM-221122/2990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				00000014410 16433	
N/A	09-Nov-2022	7.5	The DDMP/ODMF module has a service hijacking vulnerability. Successful exploit of this vulnerability may cause services to be unavailable. **CVE ID : CVE-2022-44555**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2991
N/A	09-Nov-2022	7.5	The SmartTrimProcess Event module has a vulnerability of obtaining the read and write permissions on arbitrary system files. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-44557**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2992
N/A	09-Nov-2022	5.3	The HiView module has a vulnerability of not filtering third-party apps out when the HiView module traverses to invoke the system provider. Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-HARM-221122/2993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may cause third-party apps to start periodically. **CVE ID : CVE-2022-44553**	phones-202211-00000014410 16433	
Incorrect Default Permissions	09-Nov-2022	4.3	There is a vulnerability in permission verification during the Bluetooth pairing process. Successful exploitation of this vulnerability may cause the dialog box for confirming the pairing not to be displayed during Bluetooth pairing. **CVE ID : CVE-2022-44548**	https://consumer.huawei.com/en/support/bulletin/2022/11/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202211-00000014410 16433	O-HUA-HARM-221122/2994
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Improper Neutralization of Formula Elements in a CSV File	03-Nov-2022	9.8	"IBM InfoSphere Information Server 11.7 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 223598." **CVE ID : CVE-2022-22425**	https://www.ibm.com/support/pages/node/6829953	O-IBM-AIX-221122/2995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	03-Nov-2022	9.1	"IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 236584." **CVE ID : CVE-2022-40747**	https://www.ibm.com/support/pages/node/6829373	O-IBM-AIX-221122/2996
Cross-Site Request Forgery (CSRF)	03-Nov-2022	8.8	"IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a "user that the website trusts. IBM X-Force ID: 227295. **CVE ID : CVE-2022-30608**	https://www.ibm.com/support/pages/node/6829335	O-IBM-AIX-221122/2997
Improper Neutralization of Special Elements used in an OS Command ('OS	03-Nov-2022	7.8	"IBM InfoSphere Information Server 11.7 could allow a locally authenticated attacker to execute arbitrary commands on the system by sending	https://www.ibm.com/support/pages/node/6829365	O-IBM-AIX-221122/2998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			a specially crafted request. IBM X-"Force ID: 231361. **CVE ID : CVE-2022-35717**		
Exposure of Resource to Wrong Sphere	03-Nov-2022	6.5	"IBM InfoSphere Information Server 11.7 could allow an authenticated user to access information restricted to users with elevated privileges due to improper access controls. IBM X-Force ID: 224427." **CVE ID : CVE-2022-22442**	https://www.ibm.com/support/pages/node/6829325	O-IBM-AIX-221122/2999
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/support/pages/node/6833806	O-IBM-AIX-221122/3000
Improper Input Validation	03-Nov-2022	6.5	"IBM InfoSphere Information Server 11.7 could allow a user to cause a denial of service by removing the ability to run jobs due to improper input validation.	https://www.ibm.com/support/pages/node/6829369	O-IBM-AIX-221122/3001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 235725." **CVE ID : CVE-2022-40235**		
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**	https://www.ibm.com/support/pages/node/6829907	O-IBM-AIX-221122/3002
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	"IBM InfoSphere Information Server 11.7 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: 227592. **CVE ID : CVE-2022-30615**	https://www.ibm.com/support/pages/node/6829311	O-IBM-AIX-221122/3003
Improper Neutralization of	03-Nov-2022	5.4	"IBM InfoSphere Information Server 11.7 is vulnerable	https://www.ibm.com/supp	O-IBM-AIX-221122/3004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			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: 227592." **CVE ID : CVE-2022-35642**	ort/pages/node/6829311	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	5.4	IBM WebSphere Application Server 8.5, and 9.0 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: 236588. **CVE ID : CVE-2022-40750**	https://exchange.xforce.ibmcloud.com/vulnerabilities/236588, https://www.ibm.com/support/pages/node/6833552	O-IBM-AIX-221122/3005
Product: i					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2	https://exchange.xforce.ibmcloud.com/vul	O-IBM-I-221122/3006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	nerabilities/228335, https://www.ibm.com/support/pages/node/6833806	
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**	https://www.ibm.com/support/pages/node/6829907	O-IBM-I-221122/3007
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	5.4	IBM WebSphere Application Server 8.5, and 9.0 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.	https://exchange.xforce.ibmcloud.com/vulnerabilities/236588, https://www.ibm.com/support/pages/node/6833552	O-IBM-I-221122/3008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 236588. **CVE ID : CVE-2022-40750**		
Product: linux_on_zseries					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/support/pages/node/6833806	O-IBM-LINU-221122/3009
Product: z\/os					
Affected Version(s): -					
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**	https://www.ibm.com/support/pages/node/6829907	O-IBM-Z\/O-221122/3010
Improper Neutralization of Input During	11-Nov-2022	5.4	IBM WebSphere Application Server 8.5, and 9.0 is vulnerable to cross-site scripting. This	https://exchange.xforce.ibmcloud.com/vulnerabilities/236588,	O-IBM-Z\/O-221122/3011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			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: 236588. **CVE ID : CVE-2022-40750**	https://www.ibm.com/support/pages/node/6833552	
Vendor: inhandnetworks					
Product: inrouter302_firmware					
Affected Version(s): * Up to (excluding) 3.5.56					
N/A	09-Nov-2022	9.8	The firmware of InHand Networks InRouter302 V3.5.45 introduces fixes for TALOS-2022-1472 and TALOS-2022-1474. The fixes are incomplete. An attacker can still perform, respectively, a privilege escalation and an information disclosure vulnerability. **CVE ID : CVE-2022-25932**	https://inhandnetworks.com/upload/attachment/202210/25/InHand-PSA-2022-02.pdf	O-INH-INRO-221122/3012
Product: ir302_firmware					
Affected Version(s): 3.5.45					
N/A	09-Nov-2022	8.8	A leftover debug code vulnerability exists in the	https://inhandnetworks.com/upload/att	O-INH-IR30-221122/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			console support functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-28689**	achment/202210/25/InHand-PSA-2022-02.pdf	
N/A	09-Nov-2022	8.8	A leftover debug code vulnerability exists in the console infct functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted series of network requests can lead to execution of privileged operations. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-30543**	https://inhandnetworks.com/upload/attachment/202210/25/InHand-PSA-2022-02.pdf	O-INH-IR30-221122/3014
N/A	09-Nov-2022	8.1	A leftover debug code vulnerability exists in the httpd port 4444 upload.cgi functionality of InHand Networks	https://inhandnetworks.com/upload/attachment/202210/25/InHa	O-INH-IR30-221122/3015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InRouter302 V3.5.45. A specially-crafted HTTP request can lead to arbitrary file deletion. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-29888**	nd-PSA-2022-02.pdf	
N/A	09-Nov-2022	6.5	A leftover debug code vulnerability exists in the console verify functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted series of network requests can lead to disabling security features. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-26023**	https://inhandnetworks.com/upload/attachment/202210/25/InHand-PSA-2022-02.pdf	O-INH-IR30-221122/3016
N/A	09-Nov-2022	6.5	A leftover debug code vulnerability exists in the console nvram functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted series of network requests can lead to disabling security	https://inhandnetworks.com/upload/attachment/202210/25/InHand-PSA-2022-02.pdf	O-INH-IR30-221122/3017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			features. An attacker can send a sequence of requests to trigger this vulnerability. **CVE ID : CVE-2022-29481**		
Vendor: Intel					
Product: nuc11dbbi7_firmware					
Affected Version(s): * Up to (excluding) ebtgl357.0065					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC1-221122/3018
Product: nuc11dbbi9_firmware					
Affected Version(s): * Up to (excluding) ebtgl357.0065					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC1-221122/3019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38099		
Product: nuc_10_performance_kit_nuc10i3fnhf_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3020
Product: nuc_10_performance_kit_nuc10i3fnhn_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i3fnh_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3022
Product: nuc_10_performance_kit_nuc10i3fnkn_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i3fnk_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3024
Product: nuc_10_performance_kit_nuc10i5fnhf_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i5fnhj_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3026
Product: nuc_10_performance_kit_nuc10i5fnhn_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i5fnh_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3028
Product: nuc_10_performance_kit_nuc10i5fnkn_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i5fnkp_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3030
Product: nuc_10_performance_kit_nuc10i5fnk_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i7fnhc_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3032
Product: nuc_10_performance_kit_nuc10i7fnhn_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i7fnh_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3034
Product: nuc_10_performance_kit_nuc10i7fnkn_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_kit_nuc10i7fnkp_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3036
Product: nuc_10_performance_kit_nuc10i7fnk_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_mini_pc_nuc10i3fnhfa_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3038
Product: nuc_10_performance_mini_pc_nuc10i3fnhja_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_mini_pc_nuc10i5fnhca_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3040
Product: nuc_10_performance_mini_pc_nuc10i5fnhja_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_mini_pc_nuc10i5fnkpa_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3042
Product: nuc_10_performance_mini_pc_nuc10i7fnhaa_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_10_performance_mini_pc_nuc10i7fnhja_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36789**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3044
Product: nuc_10_performance_mini_pc_nuc10i7fnkpa_firmware					
Affected Version(s): * Up to (excluding) fncml357.0053					
N/A	11-Nov-2022	7.8	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36789		
Product: nuc_11_compute_element_cm11ebc4w_firmware					
Affected Version(s): * Up to (excluding) ebtgl357.0065					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3046
Product: nuc_11_compute_element_cm11ebi38w_firmware					
Affected Version(s): * Up to (excluding) ebtgl357.0065					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3047
Product: nuc_11_compute_element_cm11ebi58w_firmware					
Affected Version(s): * Up to (excluding) ebtgl357.0065					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS	https://www.intel.com/cont	O-INT-NUC_-221122/3048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	ent/www/us/en/security-center/advisory/intel-sa-00752.html	
Product: nuc_11_compute_element_cm11ebi716w_firmware					
Affected Version(s): * Up to (excluding) ebtgl357.0065					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3049
Product: nuc_11_compute_element_cm11ebv58w_firmware					
Affected Version(s): * Up to (excluding) ebtgl357.0065					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**		
Product: nuc_11_compute_element_cm11ebv716w_firmware					
Affected Version(s): * Up to (excluding) ebtgl357.0065					
N/A	11-Nov-2022	7.8	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-38099**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3051
Product: nuc_11_performance_kit_nuc11pahi30z_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_kit_nuc11pahi3_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3053
Product: nuc_11_performance_kit_nuc11pahi50z_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_kit_nuc11pahi5_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3055
Product: nuc_11_performance_kit_nuc11pahi70z_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_kit_nuc11pahi7_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3057
Product: nuc_11_performance_kit_nuc11paki3_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_kit_nuc11paki5_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3059
Product: nuc_11_performance_kit_nuc11paki7_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_performance_mini_pc_nuc11paqi50wa_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-33176**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3061
Product: nuc_11_performance_mini_pc_nuc11paqi70qa_firmware					
Affected Version(s): * Up to (excluding) patgl357.0042					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33176		
Product: nuc_11_pro_board_nuc11tnbi30z_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3063
Product: nuc_11_pro_board_nuc11tnbi50z_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3064
Product: nuc_11_pro_board_nuc11tnbi70z_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3065
Product: nuc_11_pro_kit_nuc11tnhi30z_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3066
Product: nuc_11_pro_kit_nuc11tnhi3_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3067
Product: nuc_11_pro_kit_nuc11tnhi50z_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3068
Product: nuc_11_pro_kit_nuc11tnhi5_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for	https://www.intel.com/content/www/us/	O-INT-NUC_-221122/3069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	en/security-center/advisory/intel-sa-00752.html	
Product: nuc_11_pro_kit_nuc11tnhi70z_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3070
Product: nuc_11_pro_kit_nuc11tnki30z_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro	https://www.intel.com/content/www/us/en/security-center/adviso	O-INT-NUC_-221122/3071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	ry/intel-sa-00752.html	
Product: nuc_11_pro_kit_nuc11tnki50z_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3072
Product: nuc_11_pro_kit_nuc11tnki70z_firmware					
Affected Version(s): * Up to (excluding) tntgl357.0064					
Improper Initialization	11-Nov-2022	7.8	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37334**		
Product: nuc_8_compute_element_cm8ccb_firmware					
Affected Version(s): * Up to (excluding) cbwhl357.0096					
N/A	11-Nov-2022	6.7	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-35276**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3074
Product: nuc_8_compute_element_cm8i3cb_firmware					
Affected Version(s): * Up to (excluding) cbwhl357.0096					
N/A	11-Nov-2022	6.7	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35276		
Product: nuc_8_compute_element_cm8i5cb_firmware					
Affected Version(s): * Up to (excluding) cbwhl357.0096					
N/A	11-Nov-2022	6.7	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-35276**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3076
Product: nuc_8_compute_element_cm8i7cb_firmware					
Affected Version(s): * Up to (excluding) cbwhl357.0096					
N/A	11-Nov-2022	6.7	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-35276**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3077
Product: nuc_8_compute_element_cm8pcb_firmware					
Affected Version(s): * Up to (excluding) cbwhl357.0096					
N/A	11-Nov-2022	6.7	Improper access control in BIOS	https://www.intel.com/cont	O-INT-NUC_-221122/3078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-35276**	ent/www/us/en/security-center/advisory/intel-sa-00752.html	
Product: nuc_board_de3815tybe_firmware					
Affected Version(s): * Up to (excluding) ty0070					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC Boards, Intel(R) NUC Kits before version TY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-34152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3079
Product: nuc_board_nuc5i3mybe_firmware					
Affected Version(s): * Up to (excluding) myi30060					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow a privileged user to	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36370**		
Insecure Default Initialization of Resource	11-Nov-2022	5.5	Insecure default variable initialization in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2022-36349**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3081
Product: nuc_kit_de3815tykhe_firmware					
Affected Version(s): * Up to (excluding) ty0070					
Improper Input Validation	11-Nov-2022	6.7	Improper input validation in BIOS firmware for some Intel(R) NUC Boards, Intel(R) NUC Kits before version TY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-34152**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3082
Product: nuc_kit_nuc5i3myhe_firmware					
Affected Version(s): * Up to (excluding) myi30060					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36370**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3083
Insecure Default Initialization of Resource	11-Nov-2022	5.5	Insecure default variable initialization in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2022-36349**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3084
Product: nuc_kit_nuc5i3ryhsn_firmware					
Affected Version(s): * Up to (excluding) ry0386					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**		
Product: nuc_kit_nuc5i3ryhs_firmware					
Affected Version(s): * Up to (excluding) ry0386					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3086
Product: nuc_kit_nuc5i3ryh_firmware					
Affected Version(s): * Up to (excluding) ry0386					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3087
Product: nuc_kit_nuc5i3ryk_firmware					
Affected Version(s): * Up to (excluding) ry0386					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3088
Product: nuc_kit_nuc5i5ryhs_firmware					
Affected Version(s): * Up to (excluding) ry0386					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3089
Product: nuc_kit_nuc5i5ryh_firmware					
Affected Version(s): * Up to (excluding) ry0386					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**		
Product: nuc_kit_nuc5i5ryk_firmware					
Affected Version(s): * Up to (excluding) ry0386					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3091
Product: nuc_kit_nuc5i7ryh_firmware					
Affected Version(s): * Up to (excluding) ry0386					
Improper Authentication	11-Nov-2022	7.8	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-37345**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3092
Product: nuc_kit_wireless_adapter_driver_installer					
Affected Version(s): * Up to (excluding) 22.40.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	11-Nov-2022	7.8	Incorrect default permissions in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36377**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	O-INT-NUC_-221122/3093
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Nov-2022	7.8	Path traversal in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36400**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	O-INT-NUC_-221122/3094
Uncontrolled Search Path Element	11-Nov-2022	7.3	Uncontrolled search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	O-INT-NUC_-221122/3095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege via local access. **CVE ID : CVE-2022-36380**		
Unquoted Search Path or Element	11-Nov-2022	7.3	Unquoted search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-36384**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html	O-INT-NUC_-221122/3096
Product: nuc_m15_laptop_kit_lapbc510_firmware					
Affected Version(s): * Up to (excluding) bctgl357.0074					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Nov-2022	6.7	Improper buffer restrictions in BIOS firmware for some Intel(R) NUC M15 Laptop Kits before version BCTGL357.0074 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-32569**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3097
Product: nuc_m15_laptop_kit_lapbc710_firmware					
Affected Version(s): * Up to (excluding) bctgl357.0074					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Nov-2022	6.7	Improper buffer restrictions in BIOS firmware for some Intel(R) NUC M15 Laptop Kits before version BCTGL357.0074 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-32569**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html	O-INT-NUC_-221122/3098
Product: xmm_7560_firmware					
Affected Version(s): * Up to (excluding) m2_7560_r_01.2146.00					
Out-of-bounds Write	11-Nov-2022	9.6	Out-of-bounds write in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2022-26513**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	O-INT-XMM_-221122/3099
N/A	11-Nov-2022	8.4	Incomplete cleanup in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	O-INT-XMM_-221122/3100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege via adjacent access. **CVE ID : CVE-2022-27639**		
Improper Check for Unusual or Exceptional Conditions	11-Nov-2022	8.2	Improper conditions check in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-26079**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	O-INT-XMM_-221122/3101
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Nov-2022	8.2	Improper buffer restrictions in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-26367**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	O-INT-XMM_-221122/3102
Improper Input Validation	11-Nov-2022	8.2	Improper input validation in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	O-INT-XMM_-221122/3103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2022-28126**		
Out-of-bounds Read	11-Nov-2022	8.1	Out-of-bounds read in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via adjacent access. **CVE ID : CVE-2022-26369**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	O-INT-XMM_-221122/3104
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Nov-2022	7.2	Improper buffer restrictions in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2022-26045**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	O-INT-XMM_-221122/3105
Improper Authentication	11-Nov-2022	7.2	Improper authentication in some Intel(R) XMM(TM) 7560 Modem software before version	https://www.intel.com/content/www/us/en/security-center/adviso	O-INT-XMM_-221122/3106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2022-27874**	ry/intel-sa-00683.html	
Improper Input Validation	11-Nov-2022	7.2	Improper input validation in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2022-28611**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html	O-INT-XMM_-221122/3107
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Neutralization of Formula Elements in a CSV File	03-Nov-2022	9.8	"IBM InfoSphere Information Server 11.7 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 223598."	https://www.ibm.com/support/pages/node/6829953	O-LIN-LINU-221122/3108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22425		
Improper Restriction of XML External Entity Reference	03-Nov-2022	9.1	"IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 236584." **CVE ID : CVE-2022-40747**	https://www.ibm.com/support/pages/node/6829373	O-LIN-LINU-221122/3109
Cross-Site Request Forgery (CSRF)	03-Nov-2022	8.8	"IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a "user that the website trusts. IBM X-Force ID: 227295. **CVE ID : CVE-2022-30608**	https://www.ibm.com/support/pages/node/6829335	O-LIN-LINU-221122/3110
Improper Neutralization of Special Elements used in an	11-Nov-2022	8.8	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.2.0 could allow a remote authenticated	https://www.ibm.com/support/pages/node/6833584	O-LIN-LINU-221122/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 233786. **CVE ID : CVE-2022-38387**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Nov-2022	7.8	"IBM InfoSphere Information Server 11.7 could allow a locally authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-"Force ID: 231361. **CVE ID : CVE-2022-35717**	https://www.ibm.com/support/pages/node/6829365	O-LIN-LINU-221122/3112
N/A	09-Nov-2022	7.5	Insufficient validation of the IOCTL input buffer in AMD ?Prof may allow an attacker to send an arbitrary buffer leading to a potential Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-23831**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	O-LIN-LINU-221122/3113
N/A	09-Nov-2022	7.5	Insufficient validation in the IOCTL input/output buffer in AMD ?Prof may allow an attacker to bypass	https://www.amd.com/en/corporate/product-security/bulle	O-LIN-LINU-221122/3114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds checks potentially leading to a Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-27674**	tin/amd-sb-1046	
Insufficient Verification of Data Authenticity	09-Nov-2022	6.7	A local privilege escalation (PE) vulnerability in the Palo Alto Networks Cortex XSOAR engine software running on a Linux operating system allows a local attacker with shell access to the engine to execute programs with elevated privileges. **CVE ID : CVE-2022-0031**	https://security.paloaltonetworks.com/CVE-2022-0031	O-LIN-LINU-221122/3115
Exposure of Resource to Wrong Sphere	03-Nov-2022	6.5	"IBM InfoSphere Information Server 11.7 could allow an authenticated user to access information restricted to users with elevated privileges due to improper access controls. IBM X-Force ID: 224427." **CVE ID : CVE-2022-22442**	https://www.ibm.com/support/pages/node/6829325	O-LIN-LINU-221122/3116
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an	https://exchange.xforce.ibmcloud.com/vulnerabilities/2	O-LIN-LINU-221122/3117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	28335, https://www.ibm.com/support/pages/node/6833806	
Improper Input Validation	03-Nov-2022	6.5	"IBM InfoSphere Information Server 11.7 could allow a user to cause a denial of service by removing the ability to run jobs due to improper input validation. IBM X-Force ID: 235725." **CVE ID : CVE-2022-40235**	https://www.ibm.com/support/pages/node/6829369	O-LIN-LINU-221122/3118
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**	https://www.ibm.com/support/pages/node/6829907	O-LIN-LINU-221122/3119
NULL Pointer Dereference	10-Nov-2022	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	O-LIN-LINU-221122/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2022-34666**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	"IBM InfoSphere Information Server 11.7 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: 227592. **CVE ID : CVE-2022-30615**	https://www.ibm.com/support/pages/node/6829311	O-LIN-LINU-221122/3121
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	"IBM InfoSphere Information Server 11.7 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	https://www.ibm.com/support/pages/node/6829311	O-LIN-LINU-221122/3122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to credentials disclosure within a trusted session. IBM X-Force ID: 227592." **CVE ID : CVE-2022-35642**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	5.4	IBM Cloud Pak for Security (CP4S) 1.10.0.0 79and 1.10.2.0 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: 233663. **CVE ID : CVE-2022-36776**	https://exchange.xforce.ibmcloud.com/vulnerabilities/233663, https://www.ibm.com/support/pages/node/6833574	O-LIN-LINU-221122/3123
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	5.4	IBM WebSphere Application Server 8.5, and 9.0 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	https://exchange.xforce.ibmcloud.com/vulnerabilities/236588, https://www.ibm.com/support/pages/node/6833552	O-LIN-LINU-221122/3124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trusted session. IBM X-Force ID: 236588. **CVE ID : CVE-2022-40750**		
N/A	01-Nov-2022	0	Insertion of Sensitive Information into Log File vulnerability in Hitachi Ops Center Analyzer on Linux (Virtual Strage Software Agent component) allows local users to gain sensitive information. **CVE ID : CVE-2022-3191**	N/A	O-LIN-LINU-221122/3125
N/A	01-Nov-2022	0	Server-Side Request Forgery (SSRF) vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Data Center Analytics, Analytics probe components), Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer detail view, Hitachi Ops Center Analyzer probe components) allows Server Side Request Forgery. **CVE ID : CVE-2022-41552**	N/A	O-LIN-LINU-221122/3126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Nov-2022	0	Insertion of Sensitive Information into Temporary File vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Analytics probe component), Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer probe component) allows local users to gain sensitive information. **CVE ID : CVE-2022-41553**	N/A	O-LIN-LINU-221122/3127
Affected Version(s): * Up to (excluding) 5.19.17					
Allocation of Resources Without Limits or Throttling	04-Nov-2022	7.5	The Linux kernel NFSD implementation prior to versions 5.19.17 and 6.0.2 are vulnerable to buffer overflow. NFSD tracks the number of pages held by each NFSD thread by combining the receive and send buffers of a remote procedure call (RPC) into a single array of pages. A client can force the send buffer to shrink by sending an RPC message over TCP with	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f90497a16e434c2211c66e3de8e77b17868382b8	O-LIN-LINU-221122/3128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			garbage data added at the end of the message. The RPC message with garbage data is still correctly formed according to the specification and is passed forward to handlers. Vulnerable code in NFSD is not expecting the oversized request and writes beyond the allocated buffer space. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H **CVE ID : CVE-2022-43945**		
Affected Version(s): From (including) 6.0 Up to (excluding) 6.0.2					
Allocation of Resources Without Limits or Throttling	04-Nov-2022	7.5	The Linux kernel NFSD implementation prior to versions 5.19.17 and 6.0.2 are vulnerable to buffer overflow. NFSD tracks the number of pages held by each NFSD thread by combining the receive and send buffers of a remote procedure call (RPC) into a single array of pages. A client can force the send buffer to shrink by sending	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f90497a16e434c2211c66e3de8e77b17868382b8	O-LIN-LINU-221122/3129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an RPC message over TCP with garbage data added at the end of the message. The RPC message with garbage data is still correctly formed according to the specification and is passed forward to handlers. Vulnerable code in NFSD is not expecting the oversized request and writes beyond the allocated buffer space. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H **CVE ID : CVE-2022-43945**		
Vendor: mediatek					
Product: lr12a					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/November-2022	O-MED-LR12-221122/3130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: lr13					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-MED-LR13-221122/3131
Product: nr15					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to	https://corp.mediatek.com/product-security-bulletin/November-2022	O-MED-NR15-221122/3132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**		
Product: nr16					
Affected Version(s): -					
Reachable Assertion	08-Nov-2022	7.5	In Modem 4G RRC, there is a possible system crash due to improper input validation. This could lead to remote denial of service, when concatenating improper SIB12 (CMAS message), with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00867883; Issue ID: ALPS07274118. **CVE ID : CVE-2022-26446**	https://corp.mediatek.com/product-security-bulletin/November-2022	O-MED-NR16-221122/3133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Microsoft					
Product: azure_rtos_filex					
Affected Version(s): * Up to (excluding) 6.2.0					
Integer Overflow or Wraparound	08-Nov-2022	7.8	Azure RTOS FileX is a FAT-compatible file system thatâ€™s fully integrated with Azure RTOS ThreadX. In versions before 6.2.0, the Fault Tolerant feature of Azure RTOS FileX includes integer under and overflows which may be exploited to achieve buffer overflow and modify memory contents. When a valid log file with correct ID and checksum is detected by the `_fx_fault_tolerant_enable` function an attempt to recover the previous failed write operation is taken by call of `_fx_fault_tolerant_apply_logs`. This function iterates through the log entries and performs required recovery operations. When properly crafted a log including entries of type	https://github.com/azure-rtos/filex/security/advisories/GHSA-8jqf-wjhq-4w9f, https://github.com/azure-rtos/filex/blob/master/common/src/fx_fault_tolerant_apply_logs.c#L218	O-MIC-AZUR-221122/3134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`FX_FAULT_TOLERANT_DIR_LOG_TYPE` may be utilized to introduce unexpected behavior. This issue has been patched in version 6.2.0. A workaround to fix line 218 in fx_fault_tolerant_apply_logs.c is documented in the GHSA. **CVE ID : CVE-2022-39343**		
Product: windows					
Affected Version(s): -					
Improper Neutralization of Formula Elements in a CSV File	03-Nov-2022	9.8	"IBM InfoSphere Information Server 11.7 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 223598." **CVE ID : CVE-2022-22425**	https://www.ibm.com/support/pages/node/6829953	O-MIC-WIND-221122/3135
Improper Restriction of XML External Entity Reference	03-Nov-2022	9.1	"IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could	https://www.ibm.com/support/pages/node/6829373	O-MIC-WIND-221122/3136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 236584." **CVE ID : CVE-2022-40747**		
Cross-Site Request Forgery (CSRF)	03-Nov-2022	8.8	"IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a "user that the website trusts. IBM X-Force ID: 227295. **CVE ID : CVE-2022-30608**	https://www.ibm.com/support/pages/node/6829335	O-MIC-WIND-221122/3137
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Nov-2022	7.8	"IBM InfoSphere Information Server 11.7 could allow a locally authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-"Force ID: 231361. **CVE ID : CVE-2022-35717**	https://www.ibm.com/support/pages/node/6829365	O-MIC-WIND-221122/3138
N/A	09-Nov-2022	7.5	Insufficient validation of the IOCTL input buffer	https://www.amd.com/en/corporate/pro	O-MIC-WIND-221122/3139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in AMD ?Prof may allow an attacker to send an arbitrary buffer leading to a potential Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-23831**	duct-security/bulletin/amd-sb-1046	
N/A	09-Nov-2022	7.5	Insufficient validation in the IOCTL input/output buffer in AMD ?Prof may allow an attacker to bypass bounds checks potentially leading to a Windows kernel crash resulting in denial of service. **CVE ID : CVE-2022-27674**	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046	O-MIC-WIND-221122/3140
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-Nov-2022	7.5	Due to unsanitized NUL values, attackers may be able to maliciously set environment variables on Windows. In syscall.StartProcess and os/exec.Cmd, invalid environment variable values containing NUL values are not properly checked for. A malicious environment variable value can exploit this	https://go.dev/cl/446916, https://pkg.go.dev/vuln/GO-2022-1095, https://go.dev/issue/56284, https://groups.google.com/g/golang-announce/c/mbHY1UY3BaM/m/hSpmRzk-AgAJ	O-MIC-WIND-221122/3141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior to set a value for a different environment variable. For example, the environment variable string "A=B\x00C=D" sets the variables "A=B" and "C=D". **CVE ID : CVE-2022-41716**		
Exposure of Resource to Wrong Sphere	03-Nov-2022	6.5	"IBM InfoSphere Information Server 11.7 could allow an authenticated user to access information restricted to users with elevated privileges due to improper access controls. IBM X-Force ID: 224427." **CVE ID : CVE-2022-22442**	https://www.ibm.com/support/pages/node/6829325	O-MIC-WIND-221122/3142
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/support/pages/node/6833806	O-MIC-WIND-221122/3143
Improper Input Validation	03-Nov-2022	6.5	"IBM InfoSphere Information Server 11.7 could allow a	https://www.ibm.com/supp	O-MIC-WIND-221122/3144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to cause a denial of service by removing the ability to run jobs due to improper input validation. IBM X-Force ID: 235725." **CVE ID : CVE-2022-40235**	ort/pages/node/6829369	
Insufficiently Protected Credentials	08-Nov-2022	6.1	The Electron framework enables writing cross-platform desktop applications using JavaScript, HTML and CSS. In versions prior to 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7, Electron is vulnerable to Exposure of Sensitive Information. When following a redirect, Electron delays a check for redirecting to file:// URLs from other schemes. The contents of the file is not available to the renderer following the redirect, but if the redirect target is a SMB URL such as `file://some.website.com/`, then in some cases, Windows will connect to that	https://github.com/electron/electron/security/advisories/GHSA-p2jh-44qj-pf2v	O-MIC-WIND-221122/3145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server and attempt NTLM authentication, which can include sending hashed credentials.This issue has been patched in versions: 21.0.0-beta.1, 20.0.1, 19.0.11, and 18.3.7. Users are recommended to upgrade to the latest stable version of Electron. If upgrading isn't possible, this issue can be addressed without upgrading by preventing redirects to file:// URLs in the `WebContents.on('will-redirect')` event, for all WebContents as a workaround. **CVE ID : CVE-2022-36077**		
Improper Control of Generation of Code ('Code Injection')	08-Nov-2022	6.1	SAP GUI allows an authenticated attacker to execute scripts in the local network. On successful exploitation, the attacker can gain access to registries which can cause a limited impact on confidentiality and high impact on	https://launchpad.support.sap.com/#/notes/3237251, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	O-MIC-WIND-221122/3146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability of the application. **CVE ID : CVE-2022-41205**		
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**	https://www.ibm.com/support/pages/node/6829907	O-MIC-WIND-221122/3147
Incorrect Authorization	07-Nov-2022	5.5	Privilege escalation vulnerability in DXL Broker for Windows prior to 6.0.0.280 allows local users to gain elevated privileges by exploiting weak directory controls in the logs directory. This can lead to a denial-of-service attack on the DXL Broker. **CVE ID : CVE-2022-2188**	https://kcm.trellix.com/corporate/index?page=content&id=SB10383	O-MIC-WIND-221122/3148
NULL Pointer Dereference	10-Nov-2022	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	O-MIC-WIND-221122/3149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2022-34666**		
Improper Resource Shutdown or Release	02-Nov-2022	5.5	An improper control of a resource through its lifetime vulnerability [CWE-664] in FortiEDR CollectorWindows 4.0.0 through 4.1, 5.0.0 through 5.0.3.751, 5.1.0 may allow a privileged user to terminate the FortiEDR processes with special tools and bypass the EDR protection. **CVE ID : CVE-2022-39949**	https://fortiguard.com/psirt/FG-IR-22-218	O-MIC-WIND-221122/3150
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	"IBM InfoSphere Information Server 11.7 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.	https://www.ibm.com/support/pages/node/6829311	O-MIC-WIND-221122/3151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 227592. **CVE ID : CVE-2022-30615**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Nov-2022	5.4	"IBM InfoSphere Information Server 11.7 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: 227592." **CVE ID : CVE-2022-35642**	https://www.ibm.com/support/pages/node/6829311	O-MIC-WIND-221122/3152
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Nov-2022	5.4	IBM WebSphere Application Server 8.5, and 9.0 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: 236588.	https://exchange.xforce.ibmcloud.com/vulnerabilities/236588, https://www.ibm.com/support/pages/node/6833552	O-MIC-WIND-221122/3153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40750		
Cleartext Storage of Sensitive Information	03-Nov-2022	5.3	"IBM Robotic Process Automation 21.0.1 and 21.0.2 could disclose sensitive version information that could aid in further attacks against the system. IBM X-Force ID: 234292." **CVE ID : CVE-2022-38710**	https://www.ibm.com/support/pages/node/6831681	O-MIC-WIND-221122/3154
N/A	01-Nov-2022	0	Server-Side Request Forgery (SSRF) vulnerability in Hitachi Infrastructure Analytics Advisor on Linux (Data Center Analytics, Analytics probe components), Hitachi Ops Center Analyzer on Linux (Hitachi Ops Center Analyzer detail view, Hitachi Ops Center Analyzer probe components) allows Server Side Request Forgery. **CVE ID : CVE-2022-41552**	N/A	O-MIC-WIND-221122/3155
Product: windows_10					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	US/security-guidance/advisory/CVE-2022-41047	
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3157
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3158
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3159
Concurrent Execution using Shared Resource with	09-Nov-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/advi	O-MIC-WIND-221122/3160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	sory/CVE-2022-41088	
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3161
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3162
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3163
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41052	O-MIC-WIND-221122/3164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3165
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3166
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3167
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3168
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3170
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3171
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3172
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3173
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service	https://portal.msrc.microsof	O-MIC-WIND-221122/3174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	t.com/en-US/security-guidance/advisory/CVE-2022-41125	
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3175
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3176
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3177
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3178
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38015	guidance/advisory/CVE-2022-38015	
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3180
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3181
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3182
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3183
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security	https://portal.msrc.microsof	O-MIC-WIND-221122/3184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	t.com/en-US/security-guidance/advisory/CVE-2022-41049	
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3185
N/A	09-Nov-2022	4.6	BitLocker Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41099**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41099	O-MIC-WIND-221122/3186
N/A	11-Nov-2022	3.3	Improper access control in the Intel(R) WAPI Security software for Windows 10/11 before version 22.2150.0.1 may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2022-33973**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00720.html	O-MIC-WIND-221122/3187
Affected Version(s): 1607					
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote	https://portal.msrc.microsof	O-MIC-WIND-221122/3188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	t.com/en-US/security-guidance/advisory/CVE-2022-41047	
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3189
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3190
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3191
Concurrent Execution using Shared Resource	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	sory/CVE-2022-41088	
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3193
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3194
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3195
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				sory/CVE-2022-41052	
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3197
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3198
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3199
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3200
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41095	sory/CVE-2022-41095	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3202
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3203
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3204
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3206
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3207
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3208
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3209
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3211
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3212
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3213
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3214
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			**CVE ID : CVE-2022-41090**		
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3216
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3217
N/A	09-Nov-2022	4.6	BitLocker Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41099**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41099	O-MIC-WIND-221122/3218
Affected Version(s): 1809					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3219
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	guidance/advisory/CVE-2022-41048	
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3221
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3222
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3223
Concurrent Execution using Shared Resource	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	sory/CVE-2022-41045	
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3225
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41052	O-MIC-WIND-221122/3226
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3227
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3228
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41073	sory/CVE-2022-41073	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3230
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3231
N/A	09-Nov-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41096	O-MIC-WIND-221122/3232
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3234
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3235
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3236
N/A	09-Nov-2022	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41113**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41113	O-MIC-WIND-221122/3237
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3239
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3240
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3241
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3242
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3244
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3245
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3246
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3247
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			**CVE ID : CVE-2022-41090**		
N/A	09-Nov-2022	5.5	Windows Human Interface Device Information Disclosure Vulnerability. **CVE ID : CVE-2022-41055**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41055	O-MIC-WIND-221122/3249
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3250
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3251
N/A	09-Nov-2022	4.6	BitLocker Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41099**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41099	O-MIC-WIND-221122/3252
Affected Version(s): 20h2					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41118. **CVE ID : CVE-2022-41128**	sory/CVE-2022-41128	
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3254
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3255
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3256
Concurrent Execution using Shared Resource with Improper Synchroniz	09-Nov-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-2022-41088	O-MIC-WIND-221122/3257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**		
N/A	09-Nov-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41096	O-MIC-WIND-221122/3258
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3259
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3260
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41050	sory/CVE-2022-41050	
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41052	O-MIC-WIND-221122/3262
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3263
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3264
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3265
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41109		
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3267
N/A	09-Nov-2022	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41113**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41113	O-MIC-WIND-221122/3268
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3269
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3270
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3271
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of	https://portal.msrc.microsof	O-MIC-WIND-221122/3272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. This CVE ID is unique from CVE-2022-41109. **CVE ID : CVE-2022-41092**	t.com/en-US/security-guidance/advisory/CVE-2022-41092	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3273
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3274
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3275
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3277
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3278
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7	Windows Bind Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41114**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41114	O-MIC-WIND-221122/3279
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3280
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				sory/CVE-2022-41098	
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3282
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3283
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3284
N/A	09-Nov-2022	5.5	Windows Human Interface Device Information Disclosure Vulnerability. **CVE ID : CVE-2022-41055**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41055	O-MIC-WIND-221122/3285
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	US/security-guidance/advisory/CVE-2022-41049	
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3287
N/A	09-Nov-2022	4.6	BitLocker Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41099**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41099	O-MIC-WIND-221122/3288
Affected Version(s): 21h1					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3289
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3291
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3292
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3293
N/A	09-Nov-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41096	O-MIC-WIND-221122/3294
Concurrent Execution using	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC)	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	US/security-guidance/advisory/CVE-2022-41045	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3296
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3297
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41052	O-MIC-WIND-221122/3298
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41102. **CVE ID : CVE-2022-41101**	sory/CVE-2022-41101	
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3300
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3301
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3302
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3303
N/A	09-Nov-2022	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41113	sory/CVE-2022-41113	
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3305
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3306
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3307
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41109. **CVE ID : CVE-2022-41092**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41092	O-MIC-WIND-221122/3308
Concurrent Execution using Shared Resource with Improper	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**		
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3310
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3311
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3312
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3313
Concurrent Execution using Shared Resource with Improper Synchroniz	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			**CVE ID : CVE-2022-41118**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7	Windows Bind Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41114**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41114	O-MIC-WIND-221122/3315
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3316
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3317
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3318
Concurrent Execution using Shared Resource with	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			from CVE-2022-37992. **CVE ID : CVE-2022-41086**	sory/CVE-2022-41086	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3320
N/A	09-Nov-2022	5.5	Windows Human Interface Device Information Disclosure Vulnerability. **CVE ID : CVE-2022-41055**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41055	O-MIC-WIND-221122/3321
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3322
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	4.6	BitLocker Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41099**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41099	O-MIC-WIND-221122/3324
Affected Version(s): 21h2					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3325
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3326
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3327
Concurrent Execution using Shared Resource with	09-Nov-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/advi	O-MIC-WIND-221122/3328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	sory/CVE-2022-41039	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3329
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3330
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3332
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41052	O-MIC-WIND-221122/3333
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3334
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3335
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3337
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3338
N/A	09-Nov-2022	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41113**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41113	O-MIC-WIND-221122/3339
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3340
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3341
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	guidance/advisory/CVE-2022-37992	
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41109. **CVE ID : CVE-2022-41092**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41092	O-MIC-WIND-221122/3343
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3344
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3345
N/A	09-Nov-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41096	O-MIC-WIND-221122/3346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3347
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3348
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3349
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3350
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	7	Windows Bind Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41114**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41114	O-MIC-WIND-221122/3351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3352
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3353
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3354
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3355
N/A	09-Nov-2022	5.5	Windows Human Interface Device Information	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-41055**	US/security-guidance/advisory/CVE-2022-41055	
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3357
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3358
N/A	09-Nov-2022	4.6	BitLocker Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41099**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41099	O-MIC-WIND-221122/3359
Affected Version(s): 22h2					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3361
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3362
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3363
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41096	O-MIC-WIND-221122/3365
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3366
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3367
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3368
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote	https://portal.msrc.microsof	O-MIC-WIND-221122/3369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	t.com/en-US/security-guidance/advisory/CVE-2022-41052	
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3370
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3371
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3372
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3373
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of	https://portal.msrc.microsof	O-MIC-WIND-221122/3374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-41057**	t.com/en-US/security-guidance/advisory/CVE-2022-41057	
N/A	09-Nov-2022	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41113**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41113	O-MIC-WIND-221122/3375
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3376
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3377
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3378
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41109. **CVE ID : CVE-2022-41092**	sory/CVE-2022-41092	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3380
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3381
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3382
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3383
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT)	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	guidance/advisory/CVE-2022-41058	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3385
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7	Windows Bind Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41114**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41114	O-MIC-WIND-221122/3386
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3387
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3388
N/A	09-Nov-2022	6.5	Network Policy Server (NPS)	https://portal.msrc.microsof	O-MIC-WIND-221122/3389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	t.com/en-US/security-guidance/advisory/CVE-2022-41097	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3390
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3391
N/A	09-Nov-2022	5.5	Windows Human Interface Device Information Disclosure Vulnerability. **CVE ID : CVE-2022-41055**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41055	O-MIC-WIND-221122/3392
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41049		
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3394
N/A	09-Nov-2022	4.6	BitLocker Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41099**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41099	O-MIC-WIND-221122/3395
Product: windows_11					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3396
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3397
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	US/security-guidance/advisory/CVE-2022-41048	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3399
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3400
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3401
Concurrent Execution using Shared	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	guidance/advisory/CVE-2022-41045	
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3403
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41052	O-MIC-WIND-221122/3404
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3405
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3406
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41073	guidance/advisory/CVE-2022-41073	
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41109. **CVE ID : CVE-2022-41092**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41092	O-MIC-WIND-221122/3408
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3409
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3410
N/A	09-Nov-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41096	O-MIC-WIND-221122/3411
Concurrent Execution using	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC)	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	US/security-guidance/advisory/CVE-2022-41100	
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3413
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3414
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3415
N/A	09-Nov-2022	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41113	sory/CVE-2022-41113	
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3417
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3418
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3419
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3420
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7	Windows Bind Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41114**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41114	O-MIC-WIND-221122/3422
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3423
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3424
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3425
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3427
N/A	09-Nov-2022	5.5	Windows Human Interface Device Information Disclosure Vulnerability. **CVE ID : CVE-2022-41055**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41055	O-MIC-WIND-221122/3428
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3429
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3430
N/A	09-Nov-2022	4.6	BitLocker Security Feature Bypass Vulnerability.	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41099	US/security-guidance/advisory/CVE-2022-41099	
N/A	11-Nov-2022	3.3	Improper access control in the Intel(R) WAPI Security software for Windows 10/11 before version 22.2150.0.1 may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2022-33973**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00720.html	O-MIC-WIND-221122/3432
Affected Version(s): 22h2					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3433
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3434
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	US/security-guidance/advisory/CVE-2022-41047	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3436
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3437
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3438
Concurrent Execution using Shared Resource with	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	sory/CVE-2022-41045	
N/A	09-Nov-2022	7.8	Microsoft DWM Core Library Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41096	O-MIC-WIND-221122/3440
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3441
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3442
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41101		
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3444
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3445
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3446
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3447
N/A	09-Nov-2022	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41113**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41113	O-MIC-WIND-221122/3448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3449
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3450
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41109. **CVE ID : CVE-2022-41092**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41092	O-MIC-WIND-221122/3451
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3452
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41053	guidance/advisory/CVE-2022-41053	
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3454
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3455
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3456
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7	Windows Bind Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41114**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41114	O-MIC-WIND-221122/3457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3458
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3459
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3460
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3461
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			**CVE ID : CVE-2022-41090**		
N/A	09-Nov-2022	5.5	Windows Human Interface Device Information Disclosure Vulnerability. **CVE ID : CVE-2022-41055**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41055	O-MIC-WIND-221122/3463
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3464
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3465
N/A	09-Nov-2022	4.6	BitLocker Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-41099**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41099	O-MIC-WIND-221122/3466
Product: windows_7					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41048. **CVE ID : CVE-2022-41047**	sory/CVE-2022-41047	
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3468
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3469
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41088. **CVE ID : CVE-2022-41044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41044	O-MIC-WIND-221122/3470
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41086. **CVE ID : CVE-2022-37992**	sory/CVE-2022-37992	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3472
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3473
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3474
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3475
N/A	09-Nov-2022	6.5	Windows GDI+ Information	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	US/security-guidance/advisory/CVE-2022-41098	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3477
Affected Version(s): sp1					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3478
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3479
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3481
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3482
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3483
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3484
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3485
Concurrent Execution	09-Nov-2022	6.4	Windows Group Policy Elevation of	https://portal.msrc.microsof	O-MIC-WIND-221122/3486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	t.com/en-US/security-guidance/advisory/CVE-2022-41086	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41090. **CVE ID : CVE-2022-41116**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41116	O-MIC-WIND-221122/3487
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3488
Product: windows_8.1					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3490
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3491
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3492
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3494
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3495
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3496
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3497
Concurrent Execution using Shared Resource with Improper	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**		
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3499
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3500
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3501
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3503
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3504
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3505
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3506
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3508
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3509
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3510
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3511
Product: windows_rt_8.1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3512
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3513
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3514
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3515
Concurrent Execution using	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC)	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	US/security-guidance/advisory/CVE-2022-41045	
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3517
Product: windows_server_2008					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3518
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3519
N/A	09-Nov-2022	8.1	Windows Kerberos RC4-HMAC Elevation of	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-37966**	guidance/advisory/CVE-2022-37966	
N/A	09-Nov-2022	8.1	Netlogon RPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38023	O-MIC-WIND-221122/3521
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41088. **CVE ID : CVE-2022-41044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41044	O-MIC-WIND-221122/3522
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3523
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			**CVE ID : CVE-2022-41045**		
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3525
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3526
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3527
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3528
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3529
N/A	09-Nov-2022	7.5	Network Policy Server (NPS)	https://portal.msrc.microsof	O-MIC-WIND-221122/3530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	t.com/en-US/security-guidance/advisory/CVE-2022-41056	
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3531
N/A	09-Nov-2022	7.2	Windows Kerberos Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37967**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37967	O-MIC-WIND-221122/3532
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3533
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3534
Concurrent Execution using Shared Resource with Improper	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			**CVE ID : CVE-2022-41086**		
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3536
Affected Version(s): r2					
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3537
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3538
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	8.1	Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37966**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37966	O-MIC-WIND-221122/3540
N/A	09-Nov-2022	8.1	Netlogon RPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38023	O-MIC-WIND-221122/3541
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3542
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41088. **CVE ID : CVE-2022-41044**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41044	O-MIC-WIND-221122/3543
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41086. **CVE ID : CVE-2022-37992**	sory/CVE-2022-37992	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3545
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3546
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3547
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3548
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	guidance/advisory/CVE-2022-41109	
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3550
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3551
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3552
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3553
N/A	09-Nov-2022	7.2	Windows Kerberos Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37967	guidance/advisory/CVE-2022-37967	
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3555
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3556
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3557
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3558
Concurrent Execution	09-Nov-2022	5.9	Windows Point-to-Point Tunneling	https://portal.msrc.microsof	O-MIC-WIND-221122/3559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41090. **CVE ID : CVE-2022-41116**	t.com/en-US/security-guidance/advisory/CVE-2022-41116	
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3560
Product: windows_server_2012					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3561
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3562
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	US/security-guidance/advisory/CVE-2022-41128	
N/A	09-Nov-2022	8.1	Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37966**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37966	O-MIC-WIND-221122/3564
N/A	09-Nov-2022	8.1	Netlogon RPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38023	O-MIC-WIND-221122/3565
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3566
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			**CVE ID : CVE-2022-41088**		
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3568
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3569
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3570
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3571
Concurrent Execution using Shared Resource	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	sory/CVE-2022-41093	
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3573
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3574
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3575
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41125	sory/CVE-2022-41125	
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3577
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3578
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3579
N/A	09-Nov-2022	7.2	Windows Kerberos Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37967**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37967	O-MIC-WIND-221122/3580
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3581
N/A	09-Nov-2022	6.5	Windows GDI+ Information	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	US/security-guidance/advisory/CVE-2022-41098	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3583
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3584
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3585
Affected Version(s): r2					
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41048. **CVE ID : CVE-2022-41047**	sory/CVE-2022-41047	
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3587
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3588
N/A	09-Nov-2022	8.1	Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37966**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37966	O-MIC-WIND-221122/3589
N/A	09-Nov-2022	8.1	Netlogon RPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38023	O-MIC-WIND-221122/3590
Concurrent Execution using Shared Resource	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	sory/CVE-2022-41039	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3592
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3593
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3594
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-41057**	US/security-guidance/advisory/CVE-2022-41057	
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3596
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3597
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3598
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41100		
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3600
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3601
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3602
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3603
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3605
N/A	09-Nov-2022	7.2	Windows Kerberos Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37967**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37967	O-MIC-WIND-221122/3606
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3607
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3608
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3610
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3611
Product: windows_server_2016					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3612
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41047		
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3614
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3615
N/A	09-Nov-2022	8.1	Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37966**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37966	O-MIC-WIND-221122/3616
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	8.1	Netlogon RPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38023	O-MIC-WIND-221122/3618
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3619
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3620
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3621
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41052	sory/CVE-2022-41052	
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3623
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3624
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3625
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3626
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41095	sory/CVE-2022-41095	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3628
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3629
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3630
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092. **CVE ID : CVE-2022-41109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3632
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3633
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3634
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3635
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3636
N/A	09-Nov-2022	7.2	Windows Kerberos Elevation of	https://portal.msrc.microsof	O-MIC-WIND-221122/3637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-37967**	t.com/en-US/security-guidance/advisory/CVE-2022-37967	
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3638
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3639
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41098	O-MIC-WIND-221122/3640
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3641
Concurrent Execution using Shared	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	guidance/advisory/CVE-2022-41090	
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3643
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3644
Product: windows_server_2019					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3645
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-41048. **CVE ID : CVE-2022-41047**	sory/CVE-2022-41047	
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3647
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41039	O-MIC-WIND-221122/3648
N/A	09-Nov-2022	8.1	Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37966**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37966	O-MIC-WIND-221122/3649
Concurrent Execution using Shared Resource with Improper Synchronization	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			**CVE ID : CVE-2022-41088**		
N/A	09-Nov-2022	8.1	Netlogon RPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38023	O-MIC-WIND-221122/3651
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086. **CVE ID : CVE-2022-37992**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3652
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3653
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3654
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	US/security-guidance/advisory/CVE-2022-41052	
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3656
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41057**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41057	O-MIC-WIND-221122/3657
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3658
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3659
N/A	09-Nov-2022	7.8	Microsoft DWM Core Library Elevation of	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-41096**	guidance/advisory/CVE-2022-41096	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3661
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3662
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3663
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41109		
N/A	09-Nov-2022	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41113**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41113	O-MIC-WIND-221122/3665
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3666
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3667
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3668
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3669
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT)	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	guidance/advisory/CVE-2022-41058	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41118	O-MIC-WIND-221122/3671
N/A	09-Nov-2022	7.2	Windows Kerberos Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37967**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37967	O-MIC-WIND-221122/3672
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3673
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3674
N/A	09-Nov-2022	6.5	Windows GDI+ Information Disclosure Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41098	sory/CVE-2022-41098	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3676
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3677
N/A	09-Nov-2022	5.5	Windows Human Interface Device Information Disclosure Vulnerability. **CVE ID : CVE-2022-41055**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41055	O-MIC-WIND-221122/3678
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091. **CVE ID : CVE-2022-41049**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3680
Product: windows_server_2022					
Affected Version(s): -					
N/A	09-Nov-2022	8.8	Windows Scripting Languages Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41118. **CVE ID : CVE-2022-41128**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41128	O-MIC-WIND-221122/3681
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41048. **CVE ID : CVE-2022-41047**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41047	O-MIC-WIND-221122/3682
N/A	09-Nov-2022	8.8	Microsoft ODBC Driver Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41047. **CVE ID : CVE-2022-41048**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41048	O-MIC-WIND-221122/3683
Concurrent Execution using	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-221122/3684

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-2022-41044, CVE-2022-41088. **CVE ID : CVE-2022-41039**	US/security-guidance/advisory/CVE-2022-41039	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-41039, CVE-2022-41044. **CVE ID : CVE-2022-41088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41088	O-MIC-WIND-221122/3685
N/A	09-Nov-2022	8.1	Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37966**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37966	O-MIC-WIND-221122/3686
N/A	09-Nov-2022	8.1	Netlogon RPC Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-38023**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38023	O-MIC-WIND-221122/3687
N/A	09-Nov-2022	7.8	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41086.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37992	O-MIC-WIND-221122/3688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37992		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41093, CVE-2022-41100. **CVE ID : CVE-2022-41045**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41045	O-MIC-WIND-221122/3689
N/A	09-Nov-2022	7.8	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41050**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41050	O-MIC-WIND-221122/3690
N/A	09-Nov-2022	7.8	Windows Graphics Component Remote Code Execution Vulnerability. **CVE ID : CVE-2022-41052**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41052	O-MIC-WIND-221122/3691
N/A	09-Nov-2022	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41054**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41054	O-MIC-WIND-221122/3692
N/A	09-Nov-2022	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	O-MIC-WIND-221122/3693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41057	sory/CVE-2022-41057	
N/A	09-Nov-2022	7.8	Windows Print Spooler Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073	O-MIC-WIND-221122/3694
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41109. **CVE ID : CVE-2022-41092**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41092	O-MIC-WIND-221122/3695
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41100. **CVE ID : CVE-2022-41093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41093	O-MIC-WIND-221122/3696
N/A	09-Nov-2022	7.8	Windows Digital Media Receiver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41095	O-MIC-WIND-221122/3697
N/A	09-Nov-2022	7.8	Microsoft DWM Core Library Elevation of	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-41096**	guidance/advisory/CVE-2022-41096	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7.8	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41045, CVE-2022-41093. **CVE ID : CVE-2022-41100**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41100	O-MIC-WIND-221122/3699
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41102. **CVE ID : CVE-2022-41101**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41101	O-MIC-WIND-221122/3700
N/A	09-Nov-2022	7.8	Windows Overlay Filter Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41101. **CVE ID : CVE-2022-41102**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41102	O-MIC-WIND-221122/3701
N/A	09-Nov-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41092.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41109	O-MIC-WIND-221122/3702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41109		
N/A	09-Nov-2022	7.8	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41113**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41113	O-MIC-WIND-221122/3703
N/A	09-Nov-2022	7.8	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41125**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41125	O-MIC-WIND-221122/3704
N/A	09-Nov-2022	7.5	Windows Kerberos Denial of Service Vulnerability. **CVE ID : CVE-2022-41053**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41053	O-MIC-WIND-221122/3705
N/A	09-Nov-2022	7.5	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability. **CVE ID : CVE-2022-41056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41056	O-MIC-WIND-221122/3706
N/A	09-Nov-2022	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability. **CVE ID : CVE-2022-41058**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41058	O-MIC-WIND-221122/3707
Concurrent Execution using Shared	09-Nov-2022	7.5	Windows Scripting Languages Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-221122/3708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			CVE ID is unique from CVE-2022-41128. **CVE ID : CVE-2022-41118**	guidance/advisory/CVE-2022-41118	
N/A	09-Nov-2022	7.2	Windows Kerberos Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-37967**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37967	O-MIC-WIND-221122/3709
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	7	Windows Bind Filter Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-41114**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41114	O-MIC-WIND-221122/3710
N/A	09-Nov-2022	6.5	Windows Hyper-V Denial of Service Vulnerability. **CVE ID : CVE-2022-38015**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38015	O-MIC-WIND-221122/3711
N/A	09-Nov-2022	6.5	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability. **CVE ID : CVE-2022-41097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41097	O-MIC-WIND-221122/3712
N/A	09-Nov-2022	6.5	Windows GDI+ Information	https://portal.msrc.microsof	O-MIC-WIND-221122/3713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability. **CVE ID : CVE-2022-41098**	t.com/en-US/security-guidance/advisory/CVE-2022-41098	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	6.4	Windows Group Policy Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-37992. **CVE ID : CVE-2022-41086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41086	O-MIC-WIND-221122/3714
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Nov-2022	5.9	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-41116. **CVE ID : CVE-2022-41090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41090	O-MIC-WIND-221122/3715
N/A	09-Nov-2022	5.5	Windows Human Interface Device Information Disclosure Vulnerability. **CVE ID : CVE-2022-41055**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41055	O-MIC-WIND-221122/3716
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41091.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41049	O-MIC-WIND-221122/3717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41049		
N/A	09-Nov-2022	5.4	Windows Mark of the Web Security Feature Bypass Vulnerability. This CVE ID is unique from CVE-2022-41049. **CVE ID : CVE-2022-41091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41091	O-MIC-WIND-221122/3718
Vendor: mitshubishielectric					
Product: mac-507if-e_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-587if-e_firmware					
Affected Version(s): * Up to (including) 35.00					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-587if2-e_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-588if-e_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-002if_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-S-MA-221122/3723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Vendor: Mitsubishielectric					
Product: ma-ew85s-e_firmware					
Affected Version(s): * Up to (including) 80.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MA-E-221122/3724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MA-E-221122/3725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: ma-ew85s-uk_firmware					
Affected Version(s): * Up to (including) 80.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MA-E-221122/3726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MA-E-221122/3727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mac-507if-e_firmware					
Affected Version(s): * Up to (including) 35.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MAC--221122/3728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mac-557if-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-557if-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-558if-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: mac-558if-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-559if-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-559if-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-566ifb-e_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-567ifb-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-567ifb2-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-568if-e_firmware					
Affected Version(s): *					
Cleartext Transmission of	08-Nov-2022	9.8	Cleartext Transmission of Sensitive	https://www.mitsubishielectric.com/en/p	O-MIT-MAC--221122/3738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing	sirt/vulnerability/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-568ifb-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-568ifb2-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-568ifb3-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: mac-576if-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MAC--221122/3742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: mac-587if-e_firmware					
Affected Version(s): * Up to (including) 35.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MAC--221122/3743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mac-587if2-e_firmware					
Affected Version(s): * Up to (including) 35.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MAC--221122/3744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mac-588if-e_firmware					
Affected Version(s): * Up to (including) 35.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MAC--221122/3745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mfz-gxt50\/60\/73vfk_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MFZ--221122/3746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MFZ--221122/3747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: mfz-xt50\/60vfk_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MFZ--221122/3748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MFZ--221122/3749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msxy-fp05\/07\/10\/13\/18\/20\/24vgk-sg1_firmware					
Affected Version(s): * Up to (including) 35.00					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSXY-221122/3750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSXY-221122/3751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msy-gp10\/13\/15\/18\/20\/24vfk-sg1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSY--221122/3752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSY--221122/3753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-e2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-er2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap15\/20\/25\/35\/42\/50\/60\/71vgk-et2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap22\/25\/35\/42\/50\/60\/71\/80vgkd-a2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap22\/25\/35\/42\/50\/61\/70\/80vgkd-a1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/3763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ap25\/35\/42\/50vgk-e1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-e6_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ap25\/35\/42\/50vgk-e7_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-e8_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-en1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-en2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-en3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/3776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ap25\/35\/42\/50vgk-er1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50vgk-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50\/60\/71vgk-e3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap25\/35\/42\/50\/60\/71vgk-er3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-ap25\/35\/42\/50\/60\/71vgk-et3_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ap60\/71vgk-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ap60\/71vgk-er1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ap60\/71vgk-et1_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ay25\/35\/42\/50vgk-e1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgk-e6_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgk-er1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgk-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgk-sc1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgkp-e6_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/p	O-MIT-MSZ--221122/3801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	sirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ay25\/35\/42\/50vgkp-er1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgkp-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ay25\/35\/42\/50vgkp-sc1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-e1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-bt20\/25\/35\/50vgk-e2_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-e3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-er1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-er2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-et2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-bt20\/25\/35\/50vgk-et3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/3823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ef18\/22\/25\/35\/42\/50vgkb-e1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef18\/22\/25\/35\/42\/50vgkb-e2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef18\/22\/25\/35\/42\/50vgks-e1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef18\/22\/25\/35\/42\/50vgks-e2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-ef18\/22\/25\/35\/42\/50vgkw-e1_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef18\/22\/25\/35\/42\/50vgkw-e2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-a1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-er1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-er2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkb-et2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/3845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ef22\/25\/35\/42\/50vgks-a1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgks-er1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgks-er2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgks-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-ef22\/25\/35\/42\/50vgks-et2_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-a1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-er1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-er2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ef22\/25\/35\/42\/50vgkw-et2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-exa09\/12vak_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/3867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-eza09\/12vak_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft20\/25vfk_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ft25\/35\/50vgk-e1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft25\/35\/50vgk-e2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft25\/35\/50vgk-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft25\/35\/50vgk-sc1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ft25\/35\/50vgk-sc2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/3880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-fx20\/25vfk_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-gzt09\/12\/18vak_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-gzy09\/12\/18vfk_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33322**		
Product: msz-hr25\/35\/42\/50vfk-e6_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-hr25\/35\/42\/50\/60\/71vfk-e1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-hr25\/35\/42\/50\/60\/71vfk-er1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-hr25\/35\/42\/50\/60\/71vfk-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/p	O-MIT-MSZ--221122/3892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	sirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ky09\/12\/18vfk_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50vg2b-en1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50vg2r-en1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: msz-ln18\/25\/35\/50vg2v-en1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50vg2w-en1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50vg2w-sc1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2b-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2b-e2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2b-e3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2b-et1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2r-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2r-e2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2r-e3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2r-et1_firmware					
Affected Version(s): *					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2v-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2v-e2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2v-e3_firmware					
Affected Version(s): * Up to (including) 35.00					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2v-et1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2w-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2w-e2_firmware					
Affected Version(s): * Up to (including) 35.00					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2w-e3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2w-er1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: msz-ln18\/25\/35\/50\/60vg2w-er2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vg2w-et1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vg2w-et2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln18\/25\/35\/50\/60vgb-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vgr-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln18\/25\/35\/50\/60vgv-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: msz-ln18\/25\/35\/50\/60vgw-e1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50vg2b-en2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2b-sc1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2r-en2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2r-sc1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2v-en2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50vg2v-sc1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/3945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ln25\/35\/50vg2w-en2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-a1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2b-a2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-er1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2b-er2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-er3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-et2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2b-et3_firmware					
Affected Version(s): * Up to (including) 35.00					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2r-a1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2r-a2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/3962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ln25\/35\/50\/60vg2r-er1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2r-er2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2r-er3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2r-et2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2r-et3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2v-a1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2v-a2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2v-er1_firmware					
Affected Version(s): *					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vg2v-er2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2v-er3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/3979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-ln25\/35\/50\/60vg2v-et2_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2v-et3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2w-er3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-ln25\/35\/50\/60vg2w-et3_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**	lity/pdf/2022-011_en.pdf	
Product: msz-ln25\/35\/50\/60vgb-a1_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgb-er1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgr-a1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgr-er1_firmware					
Affected Version(s): *					
Cleartext Transmissi on of	08-Nov-2022	9.8	Cleartext Transmission of Sensitive	https://www.mitsubishielectric.com/en/p	O-MIT-MSZ--221122/3991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing	sirt/vulnerability/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgv-a1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgv-er1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-ln25\/35\/50\/60vgw-er1_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-rw25\/35\/50vg-e1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-rw25\/35\/50vg-er1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/3997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/3998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-rw25\/35\/50vg-et1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-MSZ--221122/3999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/4000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-rw25\/35\/50vg-sc1_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/4001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/4002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: msz-wx18\/20\/25vfk_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/4003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralizat	08-Nov-2022	6.1	Cross-site scripting vulnerability in	https://www.mitsubishielec	O-MIT-MSZ--221122/4004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.	tric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33322		
Product: msz-zt09\/12\/18vak_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/4005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: msz-zy09\/12\/18vfk_firmware					
Affected Version(s): * Up to (including) 35.00					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-MSZ--221122/4006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-MSZ--221122/4007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: pac-wf010-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-PAC--221122/4008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Product: pac-whs01wf-e_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier)	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-PAC--221122/4009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-002if_firmware					
Affected Version(s): * Up to (including) 35.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Nov-2022	6.1	Cross-site scripting vulnerability in Mitsubishi Electric consumer electronics products (Air Conditioning, Wi-Fi Interface, Refrigerator, HEMS adapter, Remote control with Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-011_en.pdf	O-MIT-S-MA-221122/4010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch and Air Purifier) allows a remote unauthenticated attacker to execute an malicious script on a user's browser to disclose information, etc. The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33322**		
Product: s-mac-702if-b_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-S-MA-221122/4011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information	lity/pdf/2022-010_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-702if-f_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-S-MA-221122/4012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-702if-z_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-S-MA-221122/4013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-905if_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-S-MA-221122/4014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section. **CVE ID : CVE-2022-33321**		
Product: s-mac-906if_firmware					
Affected Version(s): *					
Cleartext Transmission of Sensitive Information	08-Nov-2022	9.8	Cleartext Transmission of Sensitive Information vulnerability due to the use of Basic Authentication for HTTP connections in Mitsubishi Electric consumer electronics products (PHOTOVOLTAIC COLOR MONITOR ECO-GUIDE, HEMS adapter, Wi-Fi Interface, Air Conditioning, Induction hob, Mitsubishi Electric HEMS Energy Measurement Unit, Refrigerator, Remote control with Wi-Fi	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-010_en.pdf	O-MIT-S-MA-221122/4015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interface, BATHROOM THERMO VENTILATOR, Rice cooker, Mitsubishi Electric HEMS control adapter, Energy Recovery Ventilator, Smart Switch, Ventilating Fan, Range hood fan, Energy Measurement Unit and Air Purifier) allows a remote unauthenticated attacker to disclose information in the products or cause a denial of service (DoS) condition as a result by sniffing credential information (username and password). The wide range of models/versions of Mitsubishi Electric consumer electronics products are affected by this vulnerability. As for the affected product models/versions, see the Mitsubishi Electric's advisory which is listed in [References] section.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33321		
Vendor: Oracle					
Product: solaris					
Affected Version(s): -					
Improper Input Validation	11-Nov-2022	6.5	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335. **CVE ID : CVE-2022-31772**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228335, https://www.ibm.com/support/pages/node/6833806	O-ORA-SOLA-221122/4016
Authentication Bypass by Spoofing	03-Nov-2022	5.9	"IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Web services could allow a man-in-the-middle attacker to conduct SOAPAction spoofing to execute unwanted or unauthorized operations. IBM X-Force ID: 234762." **CVE ID : CVE-2022-38712**	https://www.ibm.com/support/pages/node/6829907	O-ORA-SOLA-221122/4017
Improper Neutralization of Input During Web Page Generation	11-Nov-2022	5.4	IBM WebSphere Application Server 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://exchange.xforce.ibmcloud.com/vulnerabilities/236588, https://www.ibm.com/supp	O-ORA-SOLA-221122/4018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 236588. **CVE ID : CVE-2022-40750**	ort/pages/node/6833552	
Vendor: Phoenixcontact					
Product: fl_mguard_centerport_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4019
Product: fl_mguard_centerport_vpn-1000_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of	15-Nov-2022	7.5	A remote, unauthenticated	N/A	O-PHO-FL_M-221122/4020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_core_tx_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue.	N/A	O-PHO-FL_M-221122/4021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3480		
Product: fl_mguard_core_tx_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4022
Product: fl_mguard_delta_tx\/tx_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from	N/A	O-PHO-FL_M-221122/4023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_delta_tx\/tx_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4024
Product: fl_mguard_gt\/gt_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC	N/A	O-PHO-FL_M-221122/4025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_gt\/gt_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4026
Product: fl_mguard_pci4000_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4027
Product: fl_mguard_pci4000_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming	N/A	O-PHO-FL_M-221122/4028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_pcie4000_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4029
Product: fl_mguard_pcie4000_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of	N/A	O-PHO-FL_M-221122/4030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_rs2000_tx\/tx-b_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4031
Product: fl_mguard_rs2000_tx\/tx_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-	N/A	O-PHO-FL_M-221122/4032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_rs2005_tx_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fl_mguard_rs4000_tx\/tx-m_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4034
Product: fl_mguard_rs4000_tx\/tx-p_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring	N/A	O-PHO-FL_M-221122/4035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_rs4000_tx\/tx_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4036
Product: fl_mguard_rs4000_tx\/tx_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0	N/A	O-PHO-FL_M-221122/4037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_rs4004_tx\/dtx_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4038
Product: fl_mguard_rs4004_tx\/dtx_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of	15-Nov-2022	7.5	A remote, unauthenticated	N/A	O-PHO-FL_M-221122/4039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: fl_mguard_smart2_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue.	N/A	O-PHO-FL_M-221122/4040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3480		
Product: fl_mguard_smart2_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-FL_M-221122/4041
Product: tc_mguard_rs2000_3g_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from	N/A	O-PHO-TC_M-221122/4042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: tc_mguard_rs2000_4g_att_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-TC_M-221122/4043
Product: tc_mguard_rs2000_4g_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC	N/A	O-PHO-TC_M-221122/4044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: tc_mguard_rs2000_4g_vzw_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-TC_M-221122/4045
Product: tc_mguard_rs4000_3g_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-TC_M-221122/4046
Product: tc_mguard_rs4000_4g_att_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming	N/A	O-PHO-TC_M-221122/4047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Product: tc_mguard_rs4000_4g_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**	N/A	O-PHO-TC_M-221122/4048
Product: tc_mguard_rs4000_4g_vzw_vpn_firmware					
Affected Version(s): * Up to (excluding) 8.9.0					
Allocation of Resources Without Limits or Throttling	15-Nov-2022	7.5	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of	N/A	O-PHO-TC_M-221122/4049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue. **CVE ID : CVE-2022-3480**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Off-by-one Error	08-Nov-2022	5.5	An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service. **CVE ID : CVE-2022-3821**	https://github.com/systemd/systemd/commit/9102c625a673a3246d7e73d8737f3494446bad4e, https://github.com/systemd/systemd/pull/23933	O-RED-ENTE-221122/4050
Affected Version(s): 9.0					
Off-by-one Error	08-Nov-2022	5.5	An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for	https://github.com/systemd/systemd/commit/9102c625a673a3246d7e73d8737f3494446bad4e, https://github	O-RED-ENTE-221122/4051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service. **CVE ID : CVE-2022-3821**	.com/systemd/systemd/pull/23933	
Product: enterprise_linux_kernel-based_virtual_machine					
Affected Version(s): -					
NULL Pointer Dereference	10-Nov-2022	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2022-34666**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	O-RED-ENTE-221122/4052
Vendor: Samsung					
Product: exynos_firmware					
Affected Version(s): -					
Out-of-bounds Read	09-Nov-2022	9.1	Improper input validation vulnerability for processing SIB12 PDU in Exynos modems prior to SMR Sep-2022 Release allows remote attacker to read out of bounds memory.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=11	O-SAM-EXYN-221122/4053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39881		
Vendor: sick					
Product: sim1000_fx_firmware					
Affected Version(s): * Up to (excluding) 1.6.0					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security risk. A fix is	https://sick.com/psirt	O-SIC-SIM1-221122/4054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SIM1000 FX Partnumber 1097816 and 1097817 with firmware version < 1.6.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. The recommended solution is to update the firmware to a version >= 1.6.0 as soon as possible. (available in SICK Support Portal) **CVE ID : CVE-2022-27585**	https://sick.com/psirt	O-SIC-SIM1-221122/4055
Product: sim1004-0p0g311_firmware					
Affected Version(s): * Up to (excluding) 2.0.0					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SIM1004 Partnumber 1098148 with firmware version < 2.0.0 allows an unprivileged	https://sick.com/psirt	O-SIC-SIM1-221122/4056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 2.0.0 as soon as possible. **CVE ID : CVE-2022-27586**		
Product: sim1004_firmware					
Affected Version(s): * Up to (excluding) 2.0.0					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password	https://sick.com/psirt	O-SIC-SIM1-221122/4057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Product: sim1012-0p0g200_firmware					
Affected Version(s): * Up to (excluding) 2.2.0					
Missing Authentication for Critical Function	01-Nov-2022	7.3	Password recovery vulnerability in SICK SIM1012 Partnumber 1098146 with firmware version < 2.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as	https://sick.com/psirt	O-SIC-SIM1-221122/4058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RecoverableUserLevel by invocating the password recovery mechanism method. The recommended solution is to update the firmware to a version >= 2.2.0 as soon as possible. (available in SICK Support Portal) **CVE ID : CVE-2022-43990**		
Product: sim1012_firmware					
Affected Version(s): * Up to (excluding) 2.2.0					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success	https://sick.com/psirt	O-SIC-SIM1-221122/4059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Product: sim2000-2p04g10_firmware					
Affected Version(s): * Up to (excluding) 1.2.0					
Missing Authentication for Critical Function	01-Nov-2022	7.3	Password recovery vulnerability in SICK SIM2x00 (ARM) Partnumber 1092673 and 1081902 with firmware version <= 1.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. The recommended solution is to update the firmware to a	https://sick.com/psirt	O-SIC-SIM2-221122/4060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version >1.2.0 as soon as possible. **CVE ID : CVE-2022-43989**		
Product: sim2000st_firmware					
Affected Version(s): -					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SIM2000ST Partnumber 2086502 and 1080579 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM2000ST. The following general security practices could mitigate the	https://sick.com/psirt	O-SIC-SIM2-221122/4061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27584**		
Affected Version(s): * Up to (excluding) 1.2.0					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the	https://sick.com/psirt	O-SIC-SIM2-221122/4062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Product: sim2000_firmware					
Affected Version(s): * Up to (excluding) 1.2.0					
Missing Authentication for Critical Function	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices	https://sick.com/psirt	O-SIC-SIM2-221122/4063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Product: sim2500-2p03g10_firmware					
Affected Version(s): * Up to (excluding) 1.2.0					
Missing Authentication for Critical Function	01-Nov-2022	7.3	Password recovery vulnerability in SICK SIM2x00 (ARM) Partnumber 1092673 and 1081902 with firmware version <= 1.2.0 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. The recommended solution is to update the firmware to a version >1.2.0 as soon as possible. **CVE ID : CVE-2022-43989**	https://sick.com/psirt	O-SIC-SIM2-221122/4064
Product: sim2500_firmware					
Affected Version(s): * Up to (excluding) 1.2.0					
Missing Authentication for	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000 (PPC) Partnumber	https://sick.com/psirt	O-SIC-SIM2-221122/4065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Product: sim4000_firmware					
Affected Version(s): *					
Missing Authentication for	01-Nov-2022	9.8	Password recovery vulnerability in SICK SICK SIM4000	https://sick.com/psirt	O-SIC-SIM4-221122/4066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			(PPC) Partnumber 1078787 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to a increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. Please make sure that you apply general security practices when operating the SIM4000. The following general security practices could mitigate the associated security risk. A fix is planned but not yet scheduled. **CVE ID : CVE-2022-27582**		
Vendor: Siemens					
Product: 6ag1151-8ab01-7ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6AG1-221122/4067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1151-8fb01-2ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6AG1-221122/4068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1314-6eh04-7ab0_firmware					
Affected Version(s): * Up to (excluding) 3.3.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6AG1-221122/4069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1315-2eh14-7ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6AG1-221122/4070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1315-2fj14-2ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6AG1-221122/4071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1317-2ek14-7ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6AG1-221122/4072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6ag1317-2fk14-2ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6AG1-221122/4073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7151-8ab01-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7151-8fb01-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7154-8ab01-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7154-8fb01-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7154-8fx00-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7314-6eh04-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.3.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7315-2eh14-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7315-2fj14-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7315-7tj10-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7317-2ek14-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7317-2fk14-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7317-7tk10-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7317-7ul10-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7318-3el01-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 6es7318-3fl01-0ab0_firmware					
Affected Version(s): * Up to (excluding) 3.2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-6ES7-221122/4088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack. **CVE ID : CVE-2022-30694**		
Product: 7kg9501-0aa01-2aa1_firmware					
Affected Version(s): * Up to (excluding) 2.50					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Session Fixation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not renew the session cookie after login/logout and also accept user defined session cookies. An attacker could overwrite the stored session cookie of a user. After the victim logged in, the attacker is given access to the user's account through the activated session. **CVE ID : CVE-2022-43398**	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	O-SIE-7KG9-221122/4089
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the Language-parameter in requests to the web interface on port	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	O-SIE-7KG9-221122/4090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device. **CVE ID : CVE-2022-43439**		
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the RecordType-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device. **CVE ID : CVE-2022-43545**	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	O-SIE-7KG9-221122/4091
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All	https://cert-portal.siemens.com/produc	O-SIE-7KG9-221122/4092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the EndTime-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device. **CVE ID : CVE-2022-43546**	tcert/pdf/ssa-570294.pdf	
Product: 7kg9501-0aa31-2aa1_firmware					
Affected Version(s): * Up to (excluding) 2.50					
Session Fixation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not renew the session cookie after login/logout and also accept user defined session cookies. An attacker could overwrite the stored session	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	O-SIE-7KG9-221122/4093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cookie of a user. After the victim logged in, the attacker is given access to the user's account through the activated session. **CVE ID : CVE-2022-43398**		
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the Language-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device. **CVE ID : CVE-2022-43439**	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	O-SIE-7KG9-221122/4094
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	O-SIE-7KG9-221122/4095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the RecordType-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device. **CVE ID : CVE-2022-43545**		
Improper Input Validation	08-Nov-2022	8.8	A vulnerability has been identified in POWER METER SICAM Q100 (All versions < V2.50), POWER METER SICAM Q100 (All versions < V2.50). Affected devices do not properly validate the EndTime-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot)	https://cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf	O-SIE-7KG9-221122/4096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or to execute arbitrary code on the device. **CVE ID : CVE-2022-43546**		
Product: simatic_drive_controller_cpu_1504d_tf_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Controller (All versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_drive_controller_cpu_1507d_tf_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_pcs_firmware					
Affected Version(s): * Up to (including) 2.1					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1211c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1212c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1212fc_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1214c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1214fc_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1214_fc_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1215c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1215fc_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1215_fc_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_1217c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1211c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1212c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1212fc_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1214c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1214fc_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1215c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1215fc_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1200_cpu_12_1217c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1507s_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1507s_f_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1508s_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1508s_f_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1510sp-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1510sp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511-1_pn_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511c-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511f-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511f-1_pn_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511t-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1511tf-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1512c-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1512c_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1512sp-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1512spf-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513-1_pn_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513f-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513f-1_pn_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1513r-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515-2_pn_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_151511c-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_151511f-1_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515f-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515f-2_pn_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515r-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515t-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1515tf-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516-3_dp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516-3_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516-3_pn\/dp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516-3_pn_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516f-3_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516f-3_pn\/dp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516pro-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516pro_f_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516t-3_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1516tf-3_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517-3_dp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517-3_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517-3_pn\/dp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517-3_pn_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517f-3_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517f-3_pn\/dp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1517tf-3_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4_dp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4_pn\/dp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4_pn\/dp_mfp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518-4_pn_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518f-4_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518f-4_pn\/dp_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518hf-4_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518t-4_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518tf-4_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_1518_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_15pro-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_15prof-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_cpu_1513pro-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-1500_cpu_cpu_1513prof-2_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-400_pn\/dp_v6_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: simatic_s7-400_pn\/dp_v7_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SIMA-221122/4183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Product: sinumerik_one_firmware					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Nov-2022	3.5	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC PC Station (All versions >= V2.1), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-1500 Software Controller (All	https://cert-portal.siemens.com/productcert/pdf/ssa-478960.pdf	O-SIE-SINU-221122/4184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC WinCC Runtime Advanced (All versions), SINUMERIK ONE (All versions), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery attack. **CVE ID : CVE-2022-30694**		
Vendor: Tenda					
Product: ac23_firmware					
Affected Version(s): 16.03.07.45_cn					
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the devName parameter in the formSetDeviceName function. **CVE ID : CVE-2022-43101**	N/A	O-TEN-AC23-221122/4185
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the timeZone parameter in the fromSetSysTime function. **CVE ID : CVE-2022-43102**	N/A	O-TEN-AC23-221122/4186
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2022-43103**	N/A	O-TEN-AC23-221122/4187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the wpapsk_crypto parameter in the fromSetWirelessRepeat function. **CVE ID : CVE-2022-43104**	N/A	O-TEN-AC23-221122/4188
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the shareSpeed parameter in the fromSetWifiGusetBasic function. **CVE ID : CVE-2022-43105**	N/A	O-TEN-AC23-221122/4189
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the schedStartTime parameter in the setSchedWifi function. **CVE ID : CVE-2022-43106**	N/A	O-TEN-AC23-221122/4190
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the time parameter in the setSmartPowerManagement function.	N/A	O-TEN-AC23-221122/4191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43107		
Out-of-bounds Write	03-Nov-2022	9.8	Tenda AC23 V16.03.07.45_cn was discovered to contain a stack overflow via the firewallEn parameter in the formSetFirewallCfg function. **CVE ID : CVE-2022-43108**	N/A	O-TEN-AC23-221122/4192
Vendor: westerndigital					
Product: my_cloud_home_duo_firmware					
Affected Version(s): * Up to (excluding) 8.11.0-113					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Nov-2022	4.3	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability was discovered via an HTTP API on Western Digital My Cloud Home; My Cloud Home Duo; and SanDisk ibi devices that could allow an attacker to abuse certain parameters to point to random locations on the file system. This could also allow the attacker to initiate the installation of custom packages at these locations. This can only be	https://www.westerndigital.com/support/product-security/wdc-22016-my-cloud-home-ibi-firmware-version-8-11-0-113	O-WES-MY_C-221122/4193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited once the attacker has been authenticated to the device. This issue affects: Western Digital My Cloud Home and My Cloud Home Duo versions prior to 8.11.0-113 on Linux; SanDisk ibi versions prior to 8.11.0-113 on Linux. **CVE ID : CVE-2022-29836**		
Product: my_cloud_home_firmware					
Affected Version(s): * Up to (excluding) 8.11.0-113					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Nov-2022	4.3	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability was discovered via an HTTP API on Western Digital My Cloud Home; My Cloud Home Duo; and SanDisk ibi devices that could allow an attacker to abuse certain parameters to point to random locations on the file system. This could also allow the attacker to initiate the installation of custom packages at these locations.	https://www.westerndigital.com/support/product-security/wdc-22016-my-cloud-home-ibi-firmware-version-8-11-0-113	O-WES-MY_C-221122/4194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This can only be exploited once the attacker has been authenticated to the device. This issue affects: Western Digital My Cloud Home and My Cloud Home Duo versions prior to 8.11.0-113 on Linux; SanDisk ibi versions prior to 8.11.0-113 on Linux. **CVE ID : CVE-2022-29836**		
Product: sandisk_ibi_firmware					
Affected Version(s): * Up to (excluding) 8.11.0-113					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Nov-2022	4.3	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability was discovered via an HTTP API on Western Digital My Cloud Home; My Cloud Home Duo; and SanDisk ibi devices that could allow an attacker to abuse certain parameters to point to random locations on the file system. This could also allow the attacker to initiate the installation of custom packages at	https://www.westerndigital.com/support/product-security/wdc-22016-my-cloud-home-ibi-firmware-version-8-11-0-113	O-WES-SAND-221122/4195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these locations. This can only be exploited once the attacker has been authenticated to the device. This issue affects: Western Digital My Cloud Home and My Cloud Home Duo versions prior to 8.11.0-113 on Linux; SanDisk ibi versions prior to 8.11.0-113 on Linux. **CVE ID : CVE-2022-29836**		
Vendor: wut					
Product: at-modem-emulator_firmware					
Affected Version(s): * Up to (excluding) 1.48					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-AT-M-221122/4196
Improper Neutralization of Input During Web Page	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated	N/A	O-WUT-AT-M-221122/4197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_20ma_firmware					
Affected Version(s): * Up to (excluding) 1.48					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unauthenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4198
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the	N/A	O-WUT-COM--221122/4199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_highspeed_100basefx_firmware					
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4200
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4201
Product: com-server_highspeed_100baselx_firmware					
Affected Version(s): * Up to (excluding) 1.76					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4202
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4203
Product: com-server_highspeed_19\"_1port_firmware					
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4205
Product: com-server_highspeed_19\"_4port_firmware					
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4207
Product: com-server_highspeed_compact_firmware					
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4208
Improper Neutralization of Input During Web Page Generation	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute	N/A	O-WUT-COM--221122/4209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_highspeed_industry_firmware					
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4210
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage	N/A	O-WUT-COM--221122/4211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42786		
Product: com-server_highspeed_isolated_firmware					
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4212
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4213
Product: com-server_highspeed_lc_firmware					
Affected Version(s): * Up to (excluding) 1.48					
Use of Insufficient	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series	https://cert.vde.com/de/ad	O-WUT-COM--221122/4214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	visories/VDE-2022-043	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4215
Product: com-server_highspeed_oem_firmware					
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account on the the device. **CVE ID : CVE-2022-42787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4217
Product: com-server_highspeed_office_1port_firmware					
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4218
Improper Neutralization of	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series	N/A	O-WUT-COM--221122/4219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_highspeed_office_4port_firmware					
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4220
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload	N/A	O-WUT-COM--221122/4221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**		
Product: com-server_highspeed_poe_3x_isolated_firmware					
Affected Version(s): * Up to (excluding) 1.48					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4222
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4223
Product: com-server_highspeed_poe_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.76					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4224
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4225
Product: com-server_highspeed_ul_firmware					
Affected Version(s): * Up to (excluding) 1.48					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker can brute force the session id and gets access to an account on the the device. **CVE ID : CVE-2022-42787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4227
Product: com-server_\+\+_firmware					
Affected Version(s): * Up to (excluding) 1.48					
Use of Insufficiently Random Values	10-Nov-2022	9.8	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. An unathenticated remote attacker can brute force the session id and gets access to an account on the the device.	https://cert.vde.com/de/advisories/VDE-2022-043	O-WUT-COM--221122/4228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42787		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Nov-2022	5.4	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage **CVE ID : CVE-2022-42786**	N/A	O-WUT-COM--221122/4229
Vendor: XEN					
Product: xen					
Affected Version(s): -					
Release of Invalid Pointer or Reference	01-Nov-2022	8.8	Xenstore: Guests can crash xenstored Due to a bug in the fix of XSA-115 a malicious guest can cause xenstored to use a wrong pointer during node creation in an error path, resulting in a crash of xenstored or a memory corruption in xenstored causing further damage. Entering the error path can be controlled by the guest e.g. by exceeding the quota	https://xenbits.xenproject.org/xsa/advisory-414.txt, http://xenbits.xen.org/xsa/advisory-414.html	O-XEN-XEN-221122/4230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value of maximum nodes per domain. **CVE ID : CVE-2022-42309**		
Missing Release of Memory after Effective Lifetime	01-Nov-2022	7.5	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g.	https://xenbits.xenproject.org/xsa/advisory-326.txt, http://xenbits.xen.org/xsa/advisory-326.html	O-XEN-XEN-221122/4231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction **CVE ID : CVE-2022-42311**		
Incomplete Cleanup	01-Nov-2022	7	Xenstore: Guests can get access to Xenstore nodes of deleted domains Access rights of Xenstore nodes are per domid. When a domain is gone, there might be Xenstore nodes left with access rights containing the domid of the removed domain. This is normally no problem, as those access right entries will be corrected when such a node is written later. There is a small time window when a new domain is created, where the access rights of a past domain with the same domid as	https://xenbits.xenproject.org/xsa/advisory-417.txt, http://xenbits.xen.org/xsa/advisory-417.html	O-XEN-XEN-221122/4232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the new one will be regarded to be still valid, leading to the new domain being able to get access to a node which was meant to be accessible by the removed domain. For this to happen another domain needs to write the node before the newly created domain is being introduced to Xenstore by dom0. **CVE ID : CVE-2022-42320**		
Allocation of Resources Without Limits or Throttling	01-Nov-2022	6.5	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations	https://xenbits.xenproject.org/xsa/advisory-326.txt, http://xenbits.xen.org/xsa/advisory-326.html	O-XEN-XEN-221122/4233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction **CVE ID : CVE-2022-42312**		
Allocation of Resources Without Limits or Throttling	01-Nov-2022	6.5	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests	https://xenbits.xenproject.org/xsa/advisory-326.txt, http://xenbits.xen.org/xsa/advisory-326.html	O-XEN-XEN-221122/4234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction **CVE ID : CVE-2022-42313**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	01-Nov-2022	6.5	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as	https://xenbits.xenproject.org/xsa/advisory-326.txt, http://xenbits.xen.org/xsa/advisory-326.html	O-XEN-XEN-221122/4235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction **CVE ID : CVE-2022-42314**		
Allocation of Resources Without Limits or Throttling	01-Nov-2022	6.5	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory	https://xenbits.xenproject.org/xsa/advisory-326.txt, http://xenbits.xen.org/xsa/advisory-326.html	O-XEN-XEN-221122/4236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			- - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction **CVE ID : CVE-2022-42315**		
Allocation of Resources Without Limits or Throttling	01-Nov-2022	6.5	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored.	https://xenbits.xenproject.org/xsa/advisory-326.txt, http://xenbits.xen.org/xsa/advisory-326.html	O-XEN-XEN-221122/4237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction **CVE ID : CVE-2022-42316**		
Allocation of Resources Without Limits or Throttling	01-Nov-2022	6.5	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which	https://xenbits.xenproject.org/xsa/advisory-326.txt, http://xenbits.xen.org/xsa/advisory-326.html	O-XEN-XEN-221122/4238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g. deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nodes inside a transaction **CVE ID : CVE-2022-42317**		
Allocation of Resources Without Limits or Throttling	01-Nov-2022	6.5	Xenstore: guests can let run xenstored out of memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Malicious guests can cause xenstored to allocate vast amounts of memory, eventually resulting in a Denial of Service (DoS) of xenstored. There are multiple ways how guests can cause large memory allocations in xenstored: - - by issuing new requests to xenstored without reading the responses, causing the responses to be buffered in memory - - by causing large number of watch events to be generated via setting up multiple xenstore watches and then e.g.	https://xenbits.xenproject.org/xsa/advisory-326.txt, http://xenbits.xen.org/xsa/advisory-326.html	O-XEN-XEN-221122/4239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deleting many xenstore nodes below the watched path - - by creating as many nodes as allowed with the maximum allowed size and path length in as many transactions as possible - - by accessing many nodes inside a transaction **CVE ID : CVE-2022-42318**		
Uncontrolled Recursion	01-Nov-2022	6.5	Xenstore: Guests can crash xenstored via exhausting the stack Xenstored is using recursion for some Xenstore operations (e.g. for deleting a sub-tree of Xenstore nodes). With sufficiently deep nesting levels this can result in stack exhaustion on xenstored, leading to a crash of xenstored. **CVE ID : CVE-2022-42321**	https://xenbits.xenproject.org/xsa/advisory-418.txt, http://xenbits.xen.org/xsa/advisory-418.html	O-XEN-XEN-221122/4240
N/A	09-Nov-2022	5.5	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040, http://www.openwall.com/l	O-XEN-XEN-221122/4241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2022-23824**	ists/oss-security/2022/11/10/2	
Missing Release of Memory after Effective Lifetime	01-Nov-2022	5.5	Xenstore: Cooperating guests can create arbitrary numbers of nodes T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Since the fix of XSA-322 any Xenstore node owned by a removed domain will be modified to be owned by Dom0. This will allow two malicious guests working together to create an arbitrary number of Xenstore nodes. This is possible by domain A letting domain B write into domain A's local Xenstore tree. Domain B can then create many nodes and reboot. The nodes created by domain B will now be owned by Dom0. By repeating this process over and over again an arbitrary number of nodes can be	https://xenbits.xenproject.org/xsa/advisory-419.txt, http://xenbits.xen.org/xsa/advisory-419.html, http://www.openwall.com/lists/oss-security/2022/11/01/9	O-XEN-XEN-221122/4242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			created, as Dom0's number of nodes isn't limited by Xenstore quota. **CVE ID : CVE-2022-42322**		
Missing Release of Memory after Effective Lifetime	01-Nov-2022	5.5	Xenstore: Cooperating guests can create arbitrary numbers of nodes T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Since the fix of XSA-322 any Xenstore node owned by a removed domain will be modified to be owned by Dom0. This will allow two malicious guests working together to create an arbitrary number of Xenstore nodes. This is possible by domain A letting domain B write into domain A's local Xenstore tree. Domain B can then create many nodes and reboot. The nodes created by domain B will now be owned by Dom0. By repeating this process over and over again an	https://xenbits.xenproject.org/xsa/advisory-419.txt, http://xenbits.xen.org/xsa/advisory-419.html, http://www.openwall.com/lists/oss-security/2022/11/01/9	O-XEN-XEN-221122/4243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary number of nodes can be created, as Dom0's number of nodes isn't limited by Xenstore quota. **CVE ID : CVE-2022-42323**		
Affected Version(s): *					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Nov-2022	5.5	Oxenstored 32->31 bit integer truncation issues Integers in Ocaml are 63 or 31 bits of signed precision. The Ocaml Xenbus library takes a C uint32_t out of the ring and casts it directly to an Ocaml integer. In 64-bit Ocaml builds this is fine, but in 32-bit builds, it truncates off the most significant bit, and then creates unsigned/signed confusion in the remainder. This in turn can feed a negative value into logic not expecting a negative value, resulting in unexpected exceptions being thrown. The unexpected exception is not handled suitably, creating a busy-loop trying (and	https://xenbits.xenproject.org/xsa/advisory-420.txt, http://xenbits.xen.org/xsa/advisory-420.html, http://www.openwall.com/lists/oss-security/2022/11/01/10	O-XEN-XEN-221122/4244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failing) to take the bad packet out of the xenstore ring. **CVE ID : CVE-2022-42324**		
Affected Version(s): 4.16					
N/A	01-Nov-2022	7.1	x86: unintended memory sharing between guests On Intel systems that support the "virtualize APIC accesses" feature, a guest can read and write the global shared xAPIC page by moving the local APIC out of xAPIC mode. Access to this shared page bypasses the expected isolation that should exist between two guests. **CVE ID : CVE-2022-42327**	https://xenbits.xenproject.org/xsa/advisory-412.txt, http://xenbits.xen.org/xsa/advisory-412.html, http://www.openwall.com/lists/oss-security/2022/11/01/3	O-XEN-XEN-221122/4245
Affected Version(s): From (including) 4.9.0 Up to (excluding) 4.13.0					
Incomplete Cleanup	01-Nov-2022	5.5	Xenstore: Guests can create orphaned Xenstore nodes By creating multiple nodes inside a transaction resulting in an error, a malicious guest can create orphaned nodes in the Xenstore data base, as the cleanup after the error will not remove all	http://xenbits.xen.org/xsa/advisory-415.html	O-XEN-XEN-221122/4246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nodes already created. When the transaction is committed after this situation, nodes without a valid parent can be made permanent in the data base. **CVE ID : CVE-2022-42310**		